ASA 8.2 : Port Redirection(Forwarding) avec nat, global, statique, et commandes access-list utilisant l'ASDM

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Diagramme du réseau
Autoriser l'accès sortant
Autoriser les hôtes internes à accéder aux réseaux externes à l'aide de NAT
Permettez à des hôtes internes Access aux réseaux extérieurs avec PAT
Restreindre l'accès des hôtes internes aux réseaux externes
Permettez le trafic entre les interfaces avec le même niveau de Sécurité
Autoriser les hôtes non approuvés à accéder à des hôtes sur votre réseau approuvé
Désactiver NAT pour des hôtes/réseaux spécifiques
Port Redirection(Forwarding) avec des commandes static
Limiter une session TCP/UDP à l'aide de la commande static
Liste d'accès basée sur le temps
Informations connexes

Introduction

Ce document décrit comment la redirection de port fonctionne sur le dispositif de sécurité adaptatif dédié Cisco (ASA) en utilisant l'ASDM. Il porte sur le contrôle d'accès du trafic par l'ASA et comment les règles de traduction fonctionnent.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- **Présentation de NAT**
- PIX/ASA 7.X : Redirection de port

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 8.2 de la gamme Cisco 5500 ASA
- Version 6.3 de Cisco ASDM

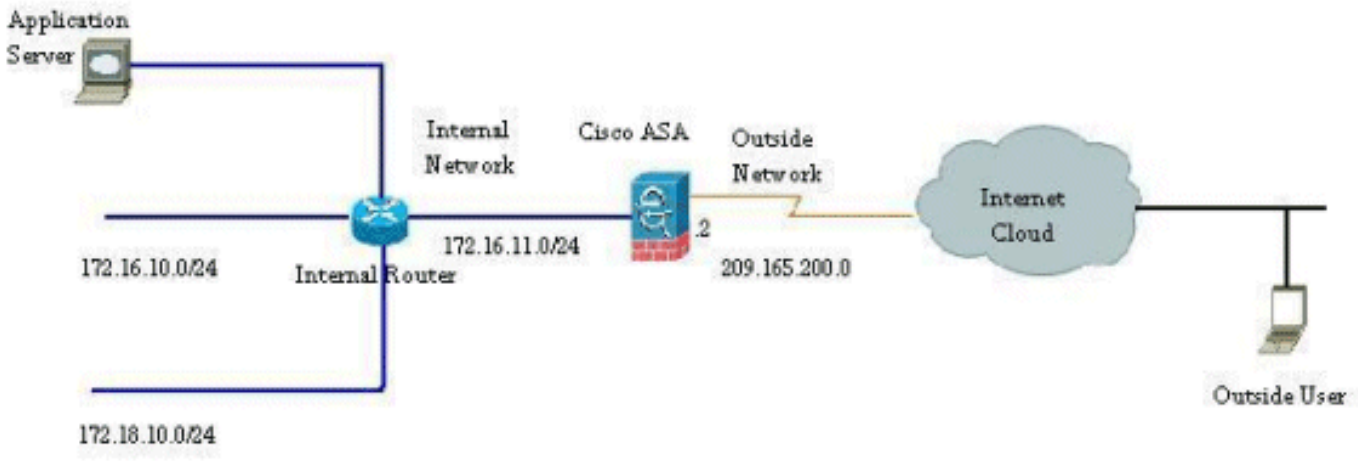
Remarque: Cette configuration fonctionne bien de la version de logiciel de Cisco ASA 8.0 8.2 seulement, parce qu'il n'y a aucun changement majeur dans la fonctionnalité NAT.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Diagramme du réseau



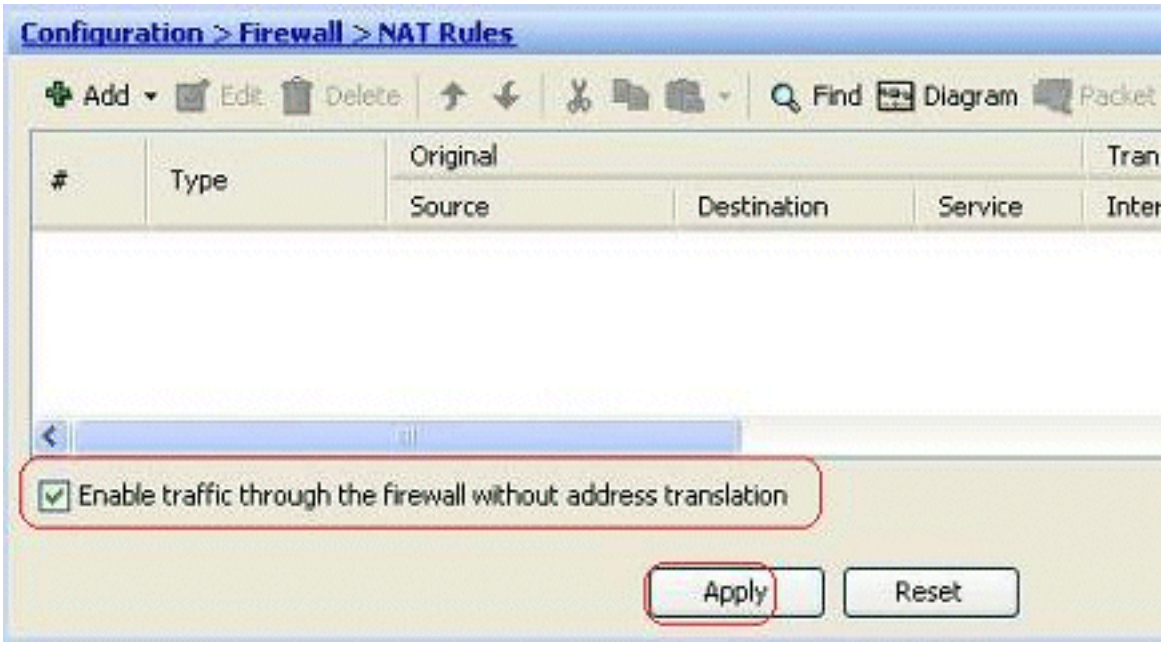
Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Autoriser l'accès sortant

L'accès sortant décrit les connexions d'une interface à niveau de sécurité plus élevé à une interface à niveau de sécurité moins élevé. Cela inclut les connexions de l'intérieur vers l'extérieur, de l'intérieur vers des zones démilitarisées (DMZ), et de DMZ vers l'extérieur. Cela peut également inclure des connexions d'une DMZ vers une autre, tant que l'interface de la source de connexion a un niveau de sécurité plus élevé que la destination.

Aucune connexion ne peut traverser les dispositifs de sécurité sans règle de conversion configurée. Cette caractéristique s'appelle le nat-control. L'image affichée ici dépeint comment désactiver ceci par l'ASDM afin de permettre des connexions par l'ASA sans n'importe quelle traduction d'adresses. Cependant, si vous faites configurer n'importe quelle règle de conversion, puis désactiver cette caractéristique ne reste pas valide pour tout le trafic et vous devrez exempter

explicitement les réseaux de la traduction d'adresses.

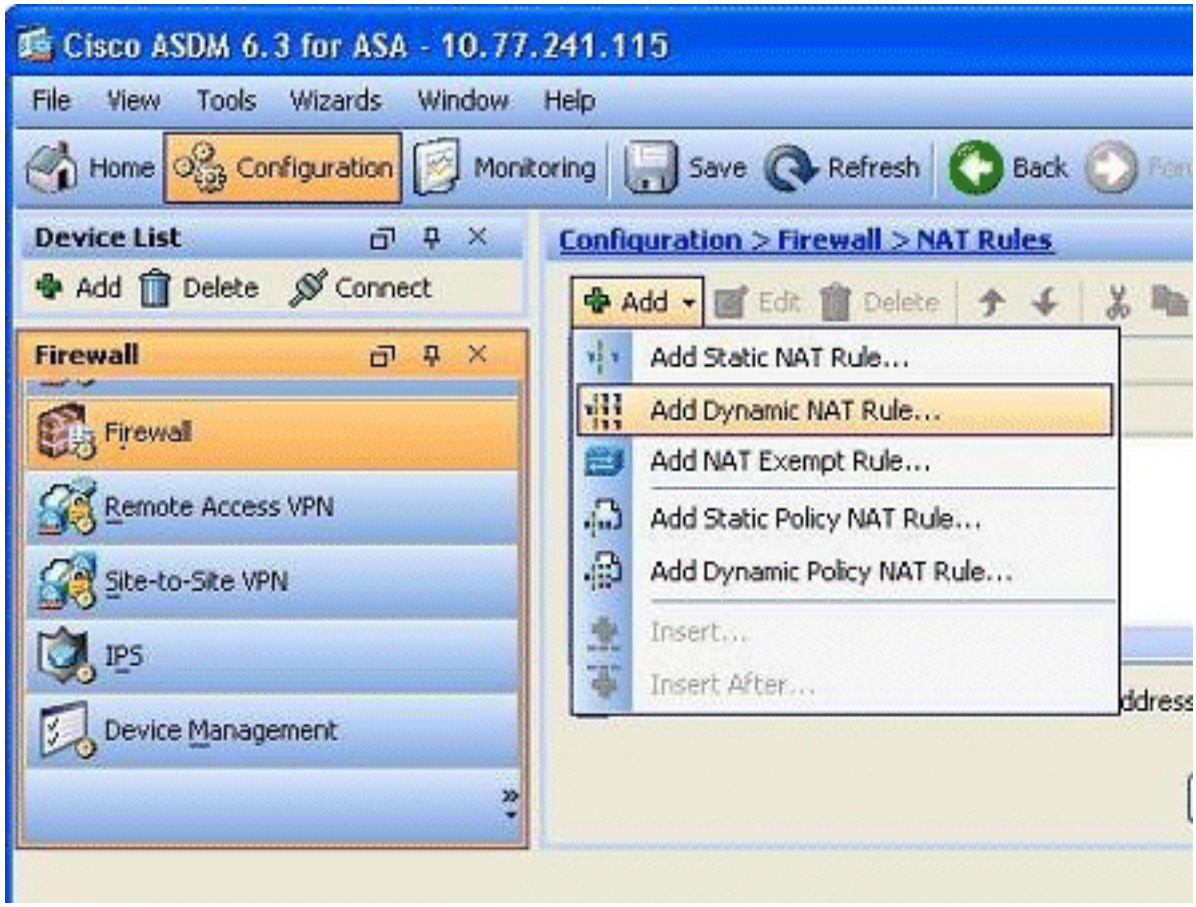


Autoriser les hôtes internes à accéder aux réseaux externes à l'aide de NAT

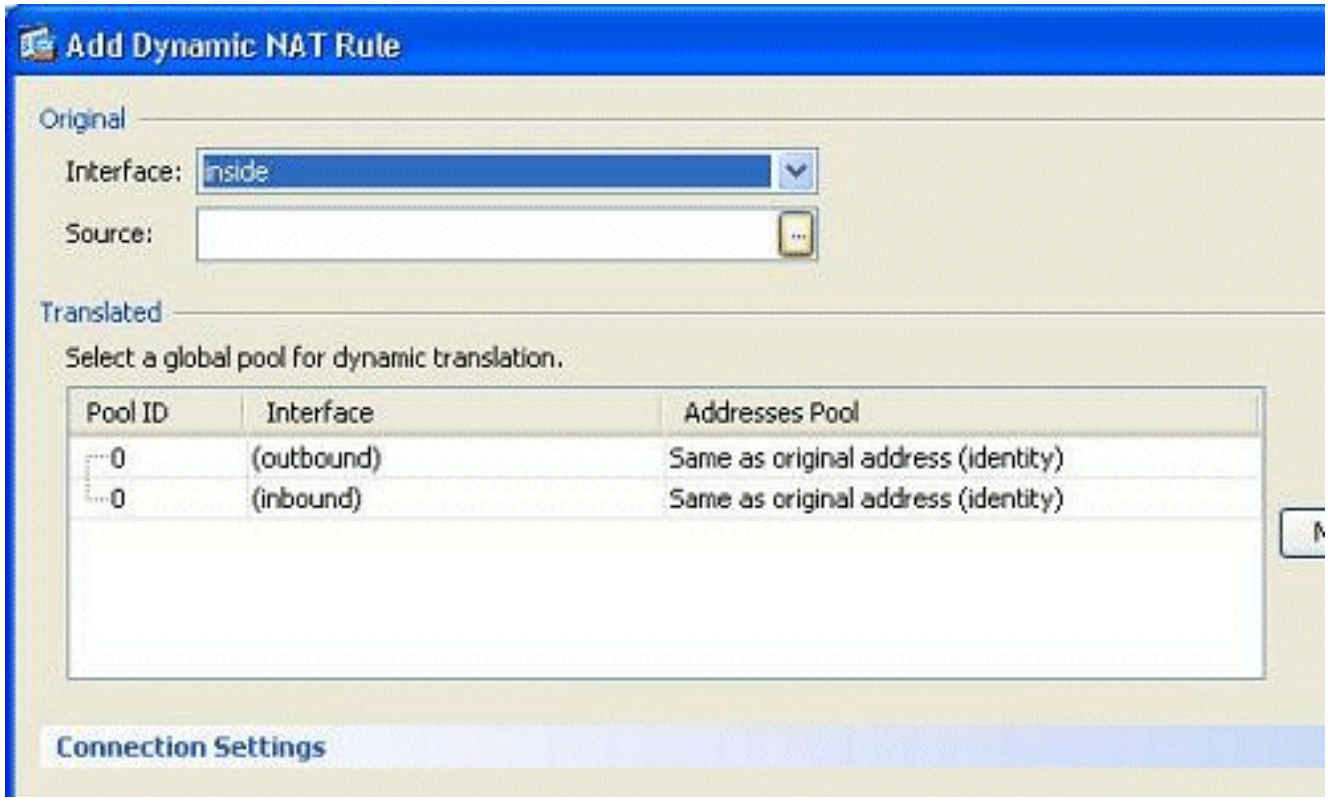
Vous pourriez permettre à un groupe d'hôtes internes/de réseaux pour accéder au monde extérieur en configurant les règles NAT dynamiques. Afin d'accomplir ceci, vous devez sélectionner la vraie adresse des hôtes/des réseaux pour donner l'accès et ils alors doivent être tracés à un groupe d'adresses IP traduites.

Terminez-vous ces étapes afin de permettre à des hôtes internes l'accès aux réseaux extérieurs avec NAT :

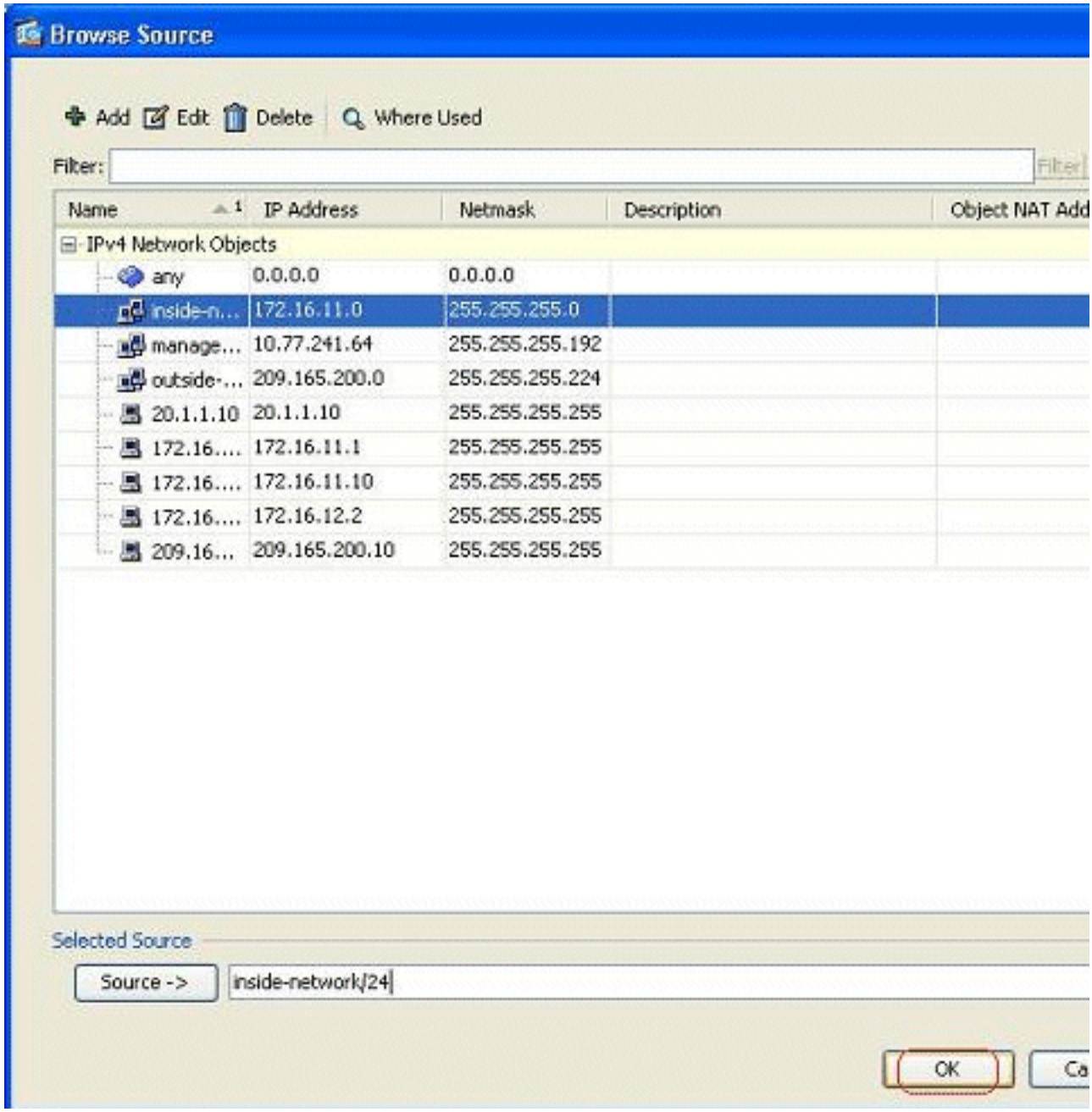
1. Allez à la **configuration** > au **Pare-feu** > aux **règles NAT**, cliquez sur Add, et puis choisissez l'option **dynamique de règle NAT d'ajouter** afin de configurer une règle NAT dynamique.



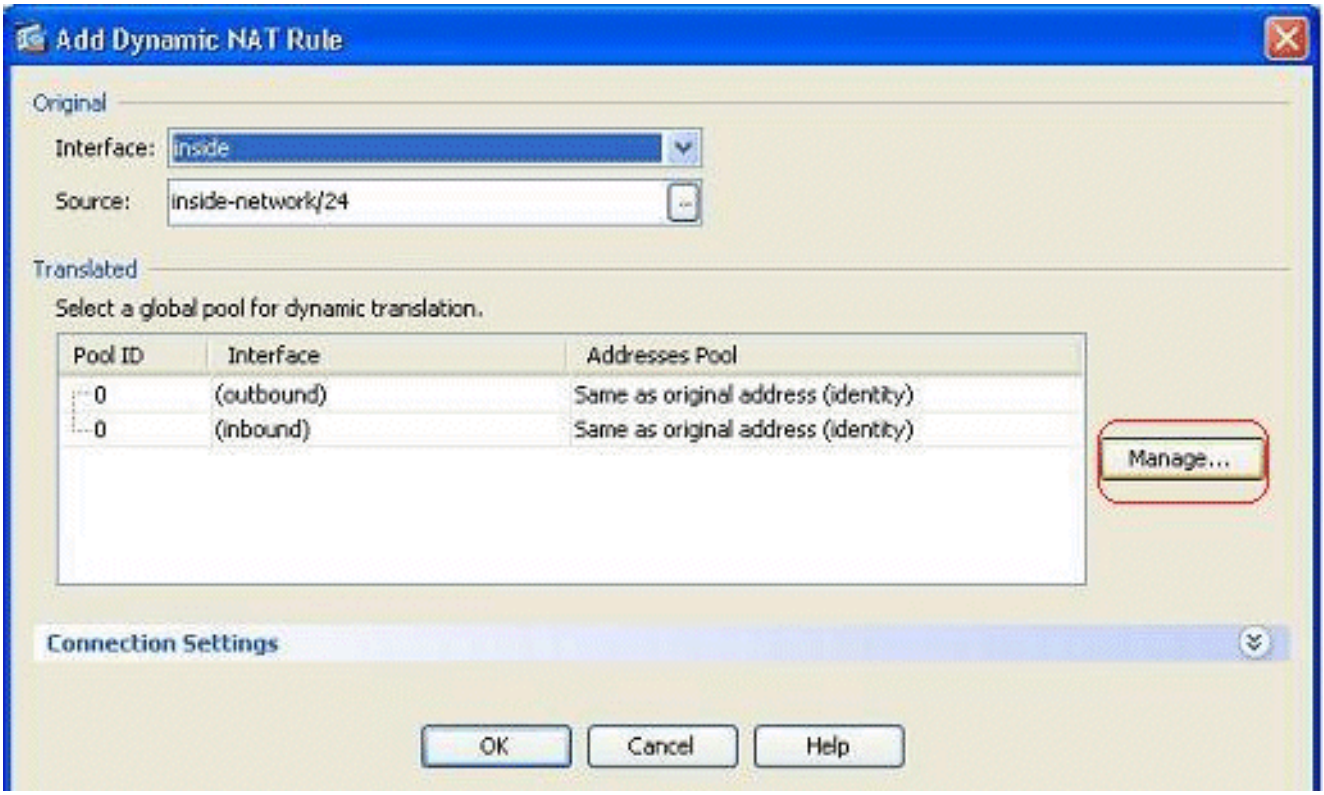
2. Choisissez le nom de l'interface à laquelle les vrais hôtes sont connectés. Choisissez la vraie adresse IP des hôtes/des réseaux utilisant les **détails** se boutonnent dans le domaine de **source**.



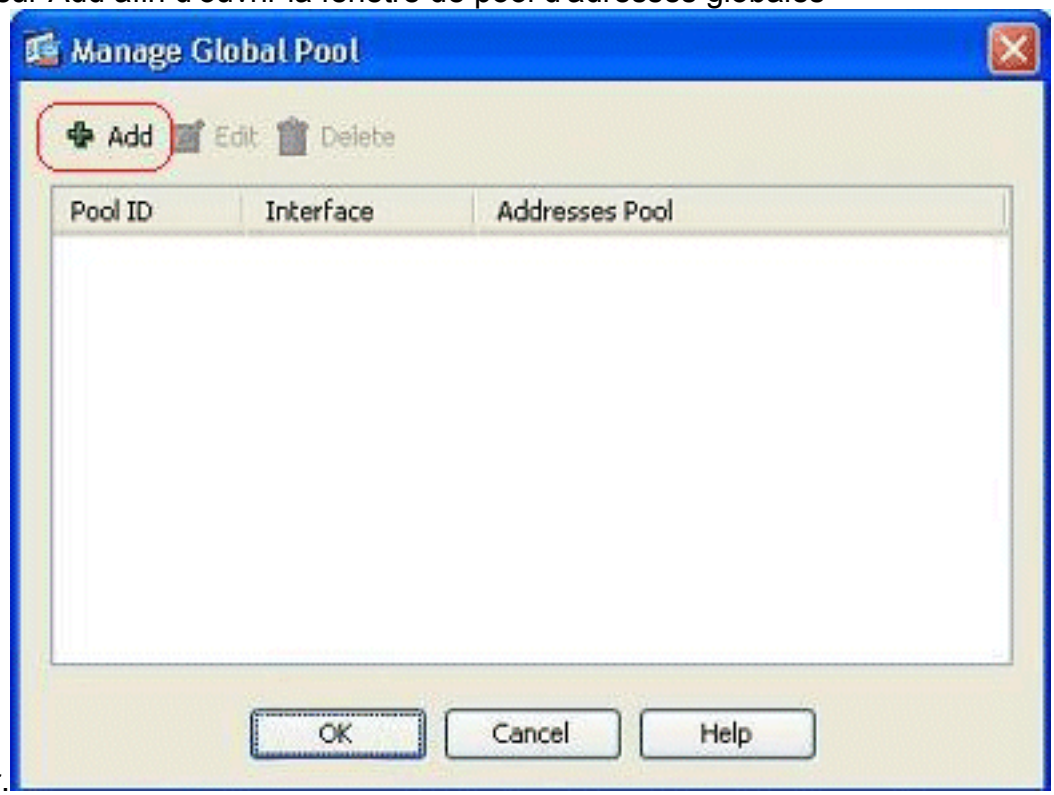
3. Dans cet exemple, l'à l'intérieur-*réseau* entier a été sélectionné. Cliquez sur OK afin de se terminer la
sélection.



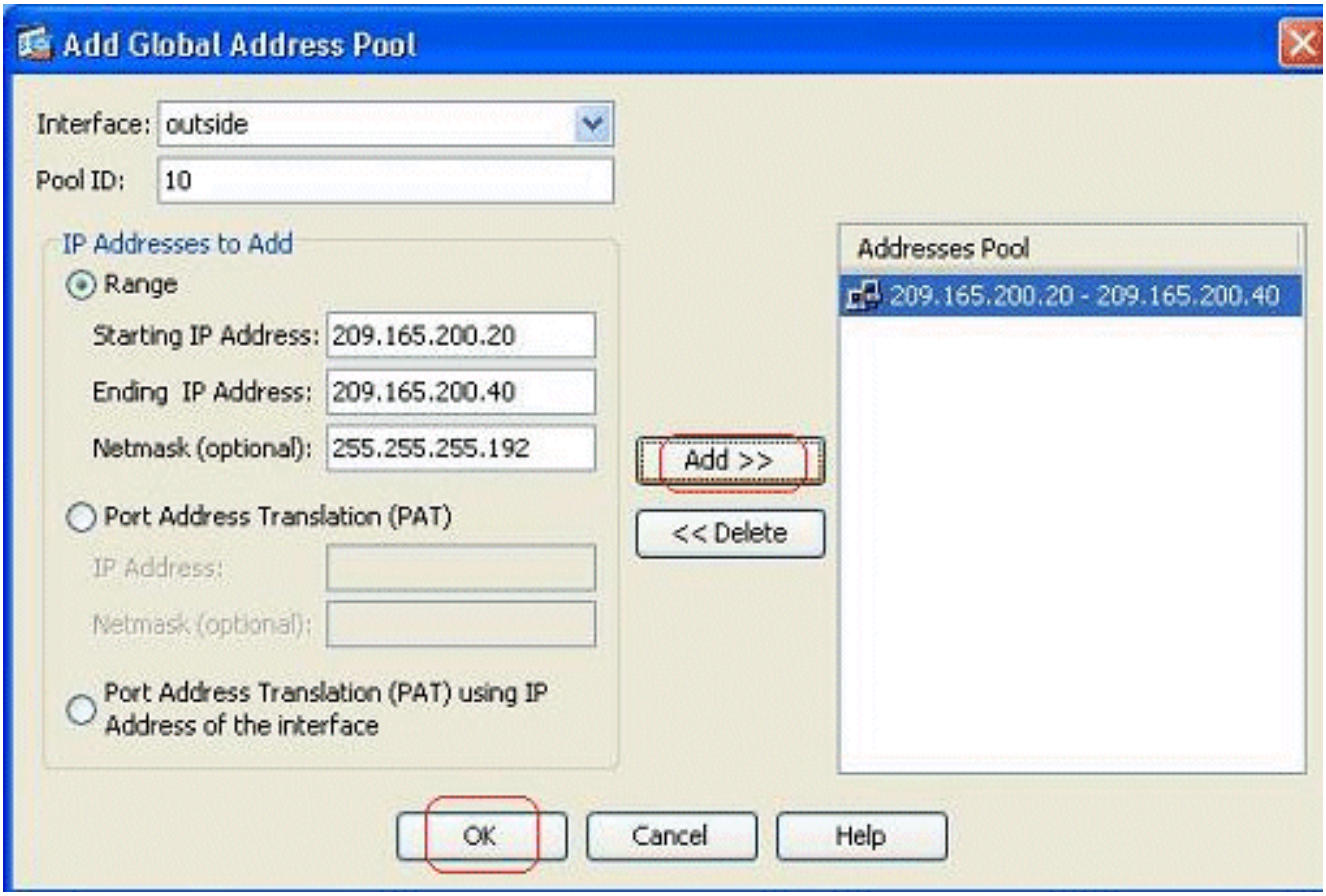
4. Le clic **parviennent** afin de sélectionner le groupe d'adresses IP auxquelles le réseau réel sera
tracé.



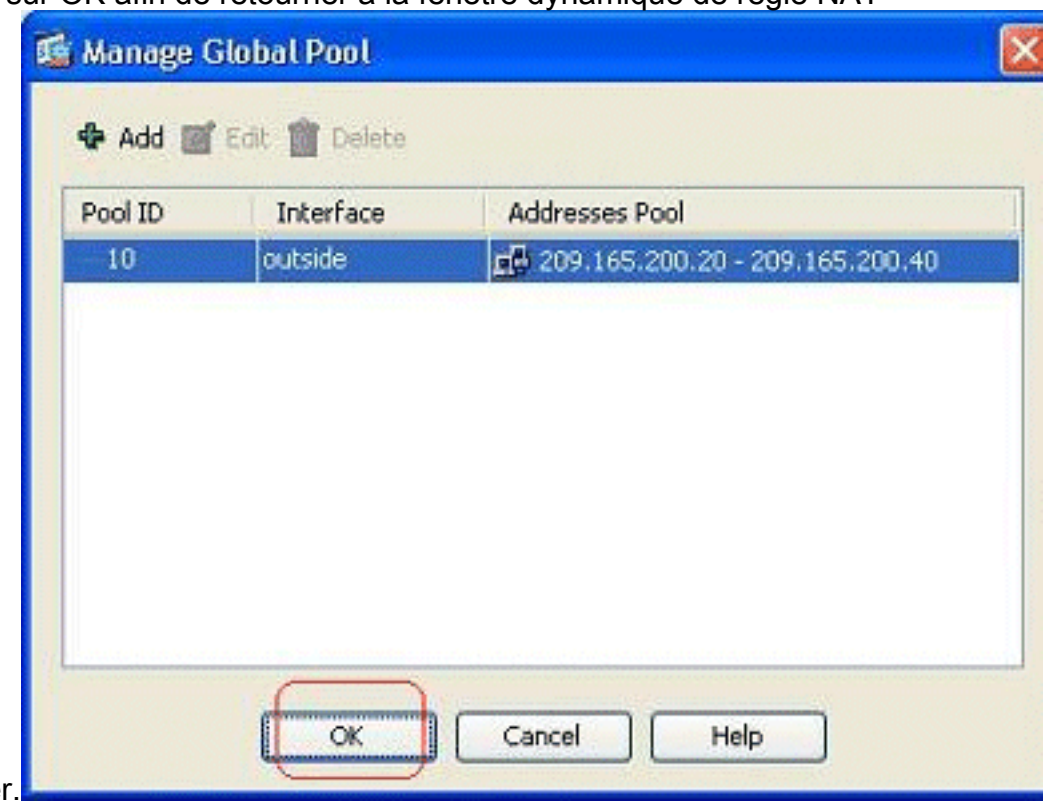
5. Cliquez sur Add afin d'ouvrir la fenêtre de pool d'adresses globales d'ajouter.



6. Choisissez l'option de **plage** et spécifiez les adresses IP commençantes et finissantes avec l'interface de sortie. En outre, spécifiez un seul ID de groupe et cliquez sur Add afin d'ajouter ces derniers au pool d'adresses. Cliquez sur OK afin de retourner à la fenêtre de pool global de
gérer.

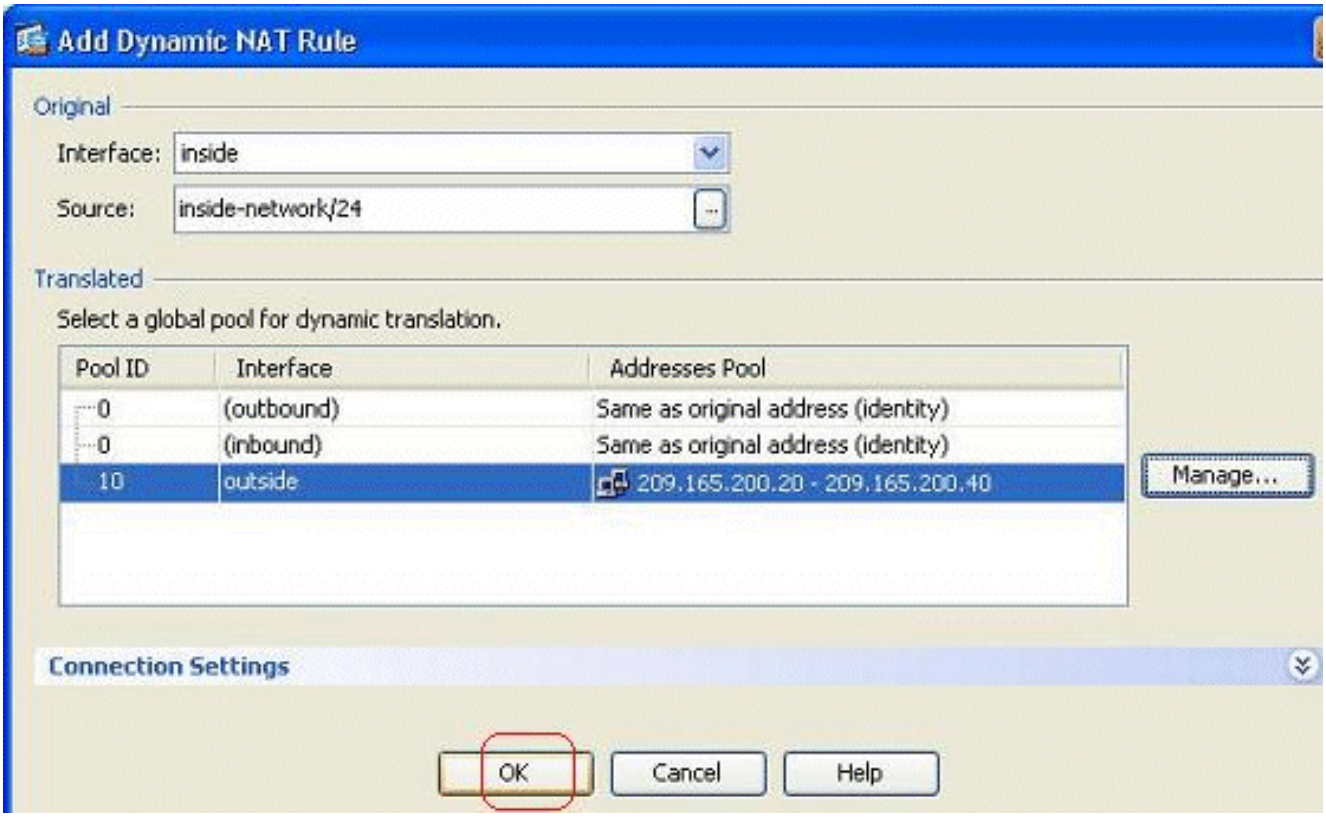


7. Cliquez sur OK afin de retourner à la fenêtre dynamique de règle NAT

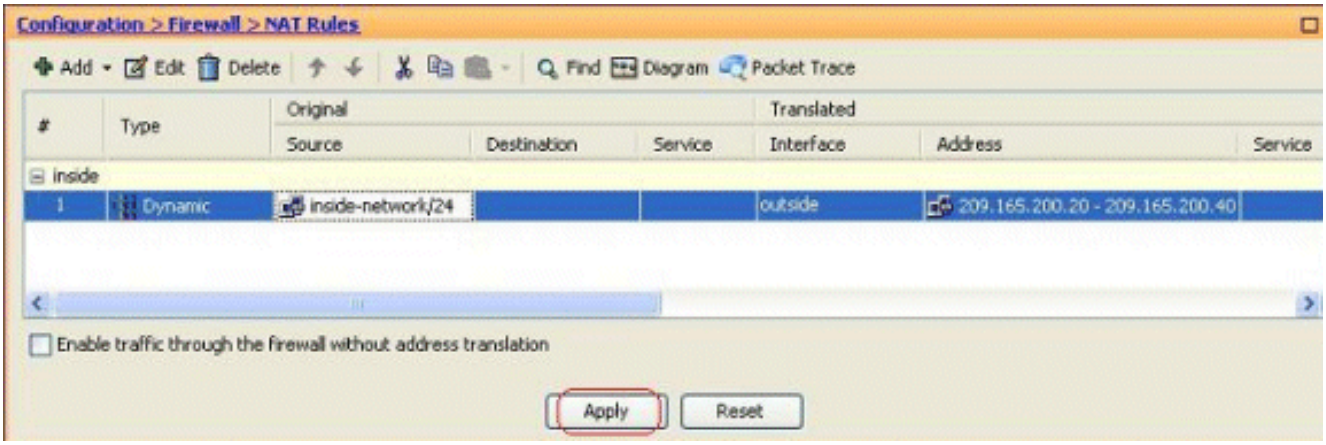


d'ajouter.

8. Cliquez sur OK afin de se terminer la configuration dynamique de règle NAT.



9. Cliquez sur Apply pour les modifications pour le prendre effet.**Remarque:** L'option d'**Enable traffic through the firewall without address translation** est décochée.



C'est le CLI équivalent sorti pour cette configuration ASDM :

```
nat-control global (outside) 10 209.165.200.20-209.165.200.40 netmask 255.255.255.192 nat
(inside) 10 172.16.11.0 255.255.255.0
```

Selon cette configuration, les hôtes dans le réseau de 172.16.11.0 obtiendront traduit à n'importe quelle adresse IP du groupe NAT, 209.165.200.20-209.165.200.40. Ici, l'ID NAT de groupe est très important. Vous pourriez affecter le même groupe NAT à un autre réseau interne/dmz. Si le groupe tracé a moins d'adresses que le vrai groupe, vous pourriez manquer d'adresses si le niveau de trafic est davantage que prévu. En conséquence, vous pourriez essayer mettre en application PAT ou vous pourriez essayer d'éditer le pool d'adresses existant pour l'étendre.

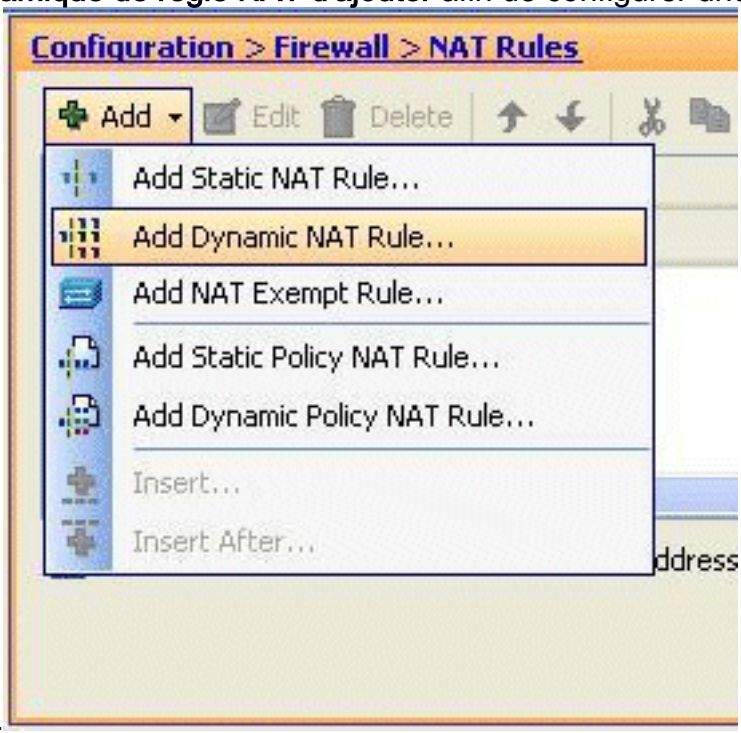
Remarque: Tout en apportant n'importe quelle modification à la règle de traduction existante, notez que vous devez utiliser la commande de clear xlate pour que ces modifications les prennent effet. Autrement, la connexion existante précédente demeurera là dans la table de connexion jusqu'à eux minuterie. Soyez prudent en utilisant la commande de **clear xlate**, parce qu'elle termine immédiatement les connexions existantes.

Permettez à des hôtes internes Access aux réseaux extérieurs avec PAT

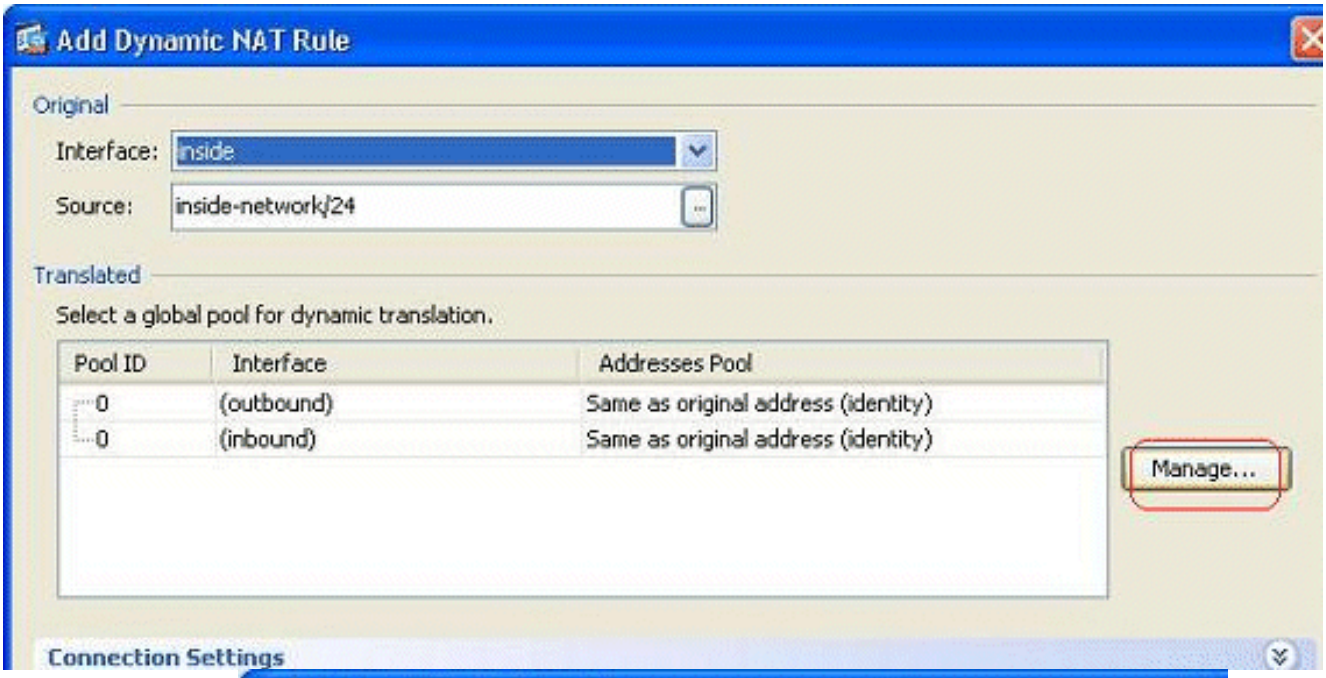
Si vous voulez que les hôtes internes partagent une seule adresse publique pour la traduction, utilisez PAT. Si l'instruction **global** spécifie une adresse, cette adresse est une traduction de port. L'ASA permet une traduction de port par supports d'interface et de cette traduction jusqu'à 65,535 objets xlate actifs à l'adresse globale simple.

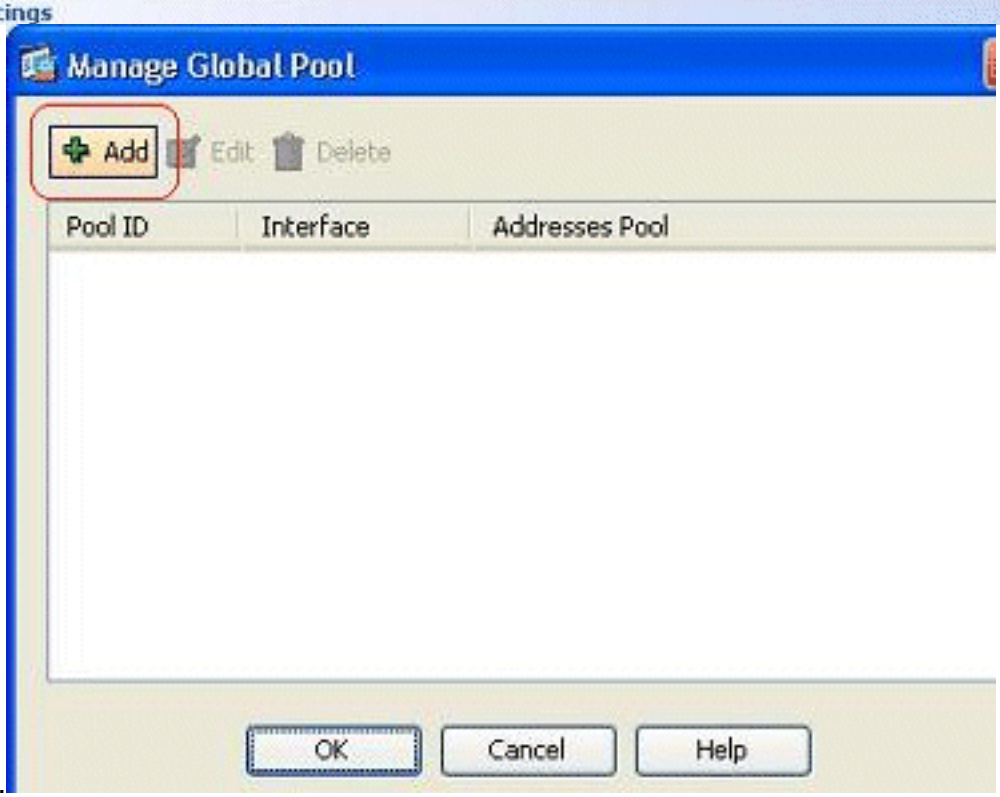
Terminez-vous ces étapes afin de permettre à des hôtes internes l'accès aux réseaux extérieurs avec PAT :

1. Allez à la **configuration** > au **Pare-feu** > aux **règles NAT**, cliquez sur Add, et puis choisissez l'option **dynamique de règle NAT d'ajouter** afin de configurer une règle NAT dynamique.

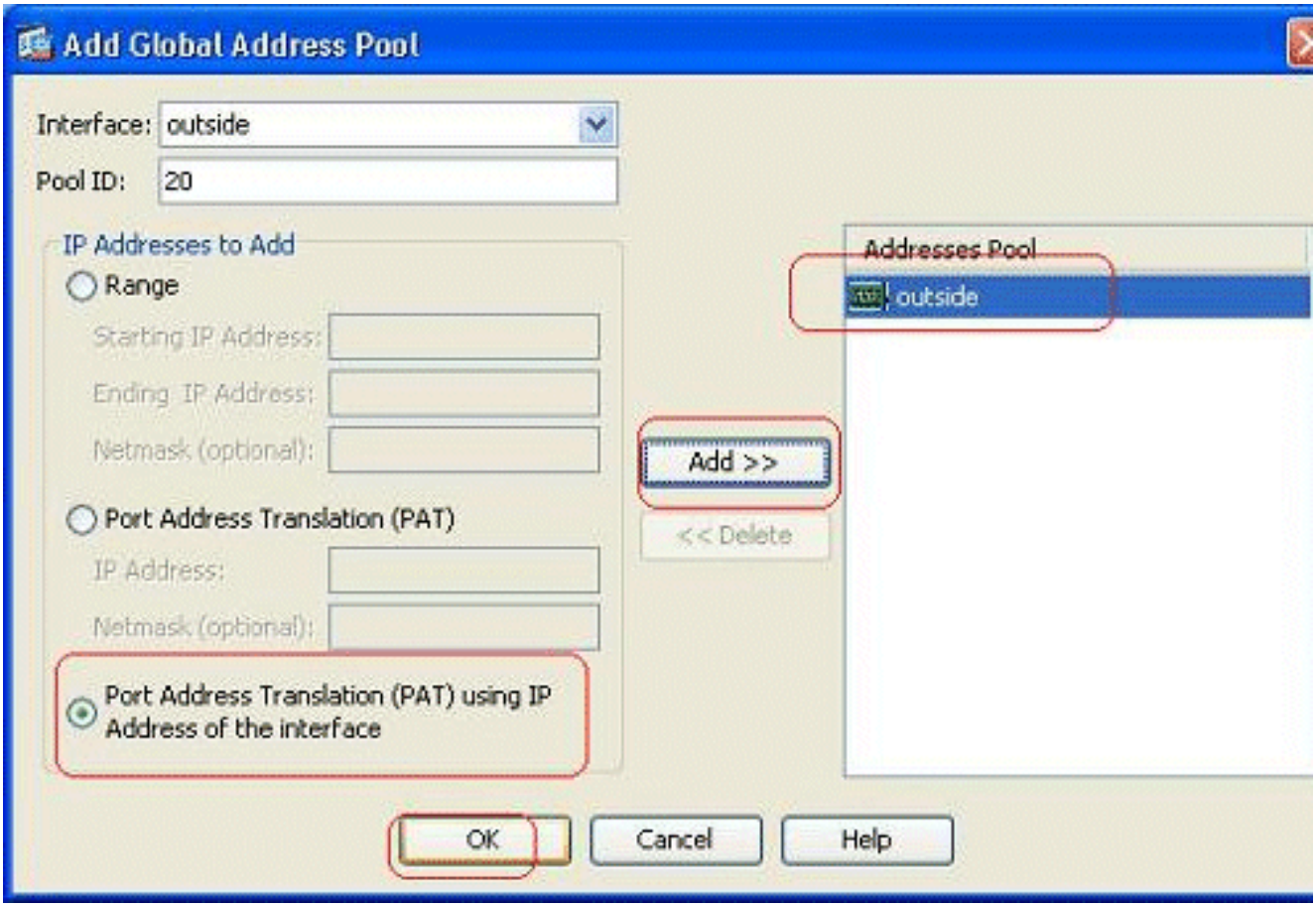


2. Choisissez le nom de l'interface à laquelle les vrais hôtes sont connectés. Choisissez la vraie adresse IP des hôtes/des réseaux utilisant les **détails** se boutonnent dans le domaine de **source**, et choisissent l'à l'intérieur-**réseau**. Le clic **parviennent** afin de définir les informations d'adresse
traduites.

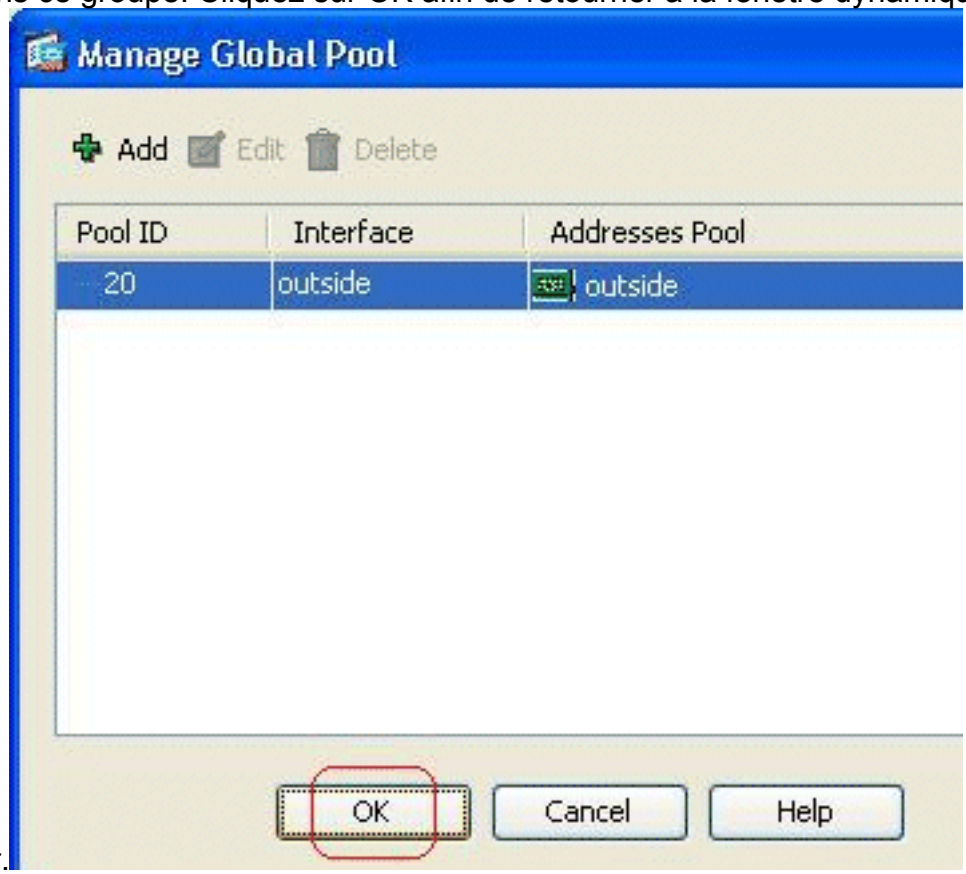




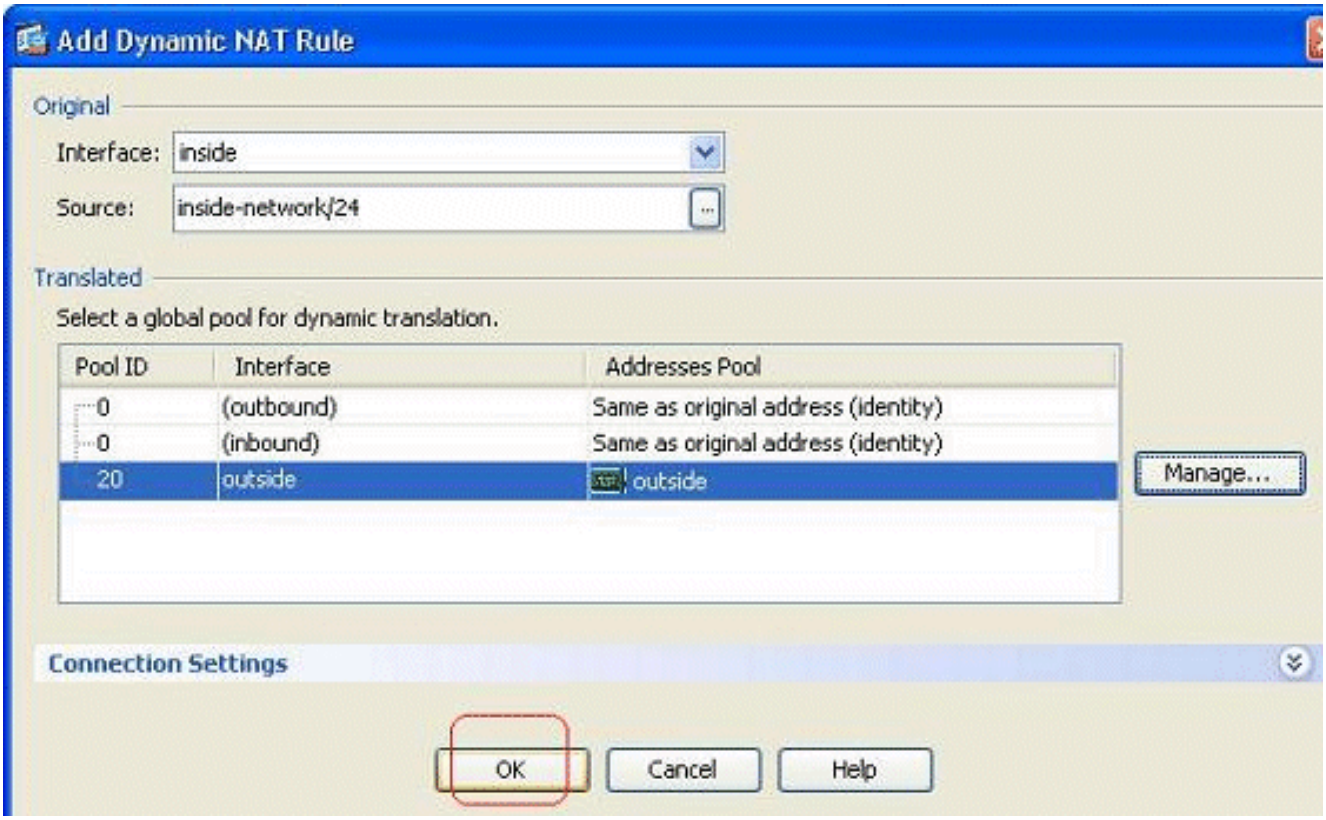
3. Cliquez sur **Add**.
4. Choisissez la **translation d'adresses d'adresse du port (PAT) utilisant l'adresse IP de l'**option d'**interface**, et cliquez sur Add afin de l'ajouter au pool d'adresses. N'oubliez pas d'assigner un identificateur unique pour ce pool d'adresses
NAT.



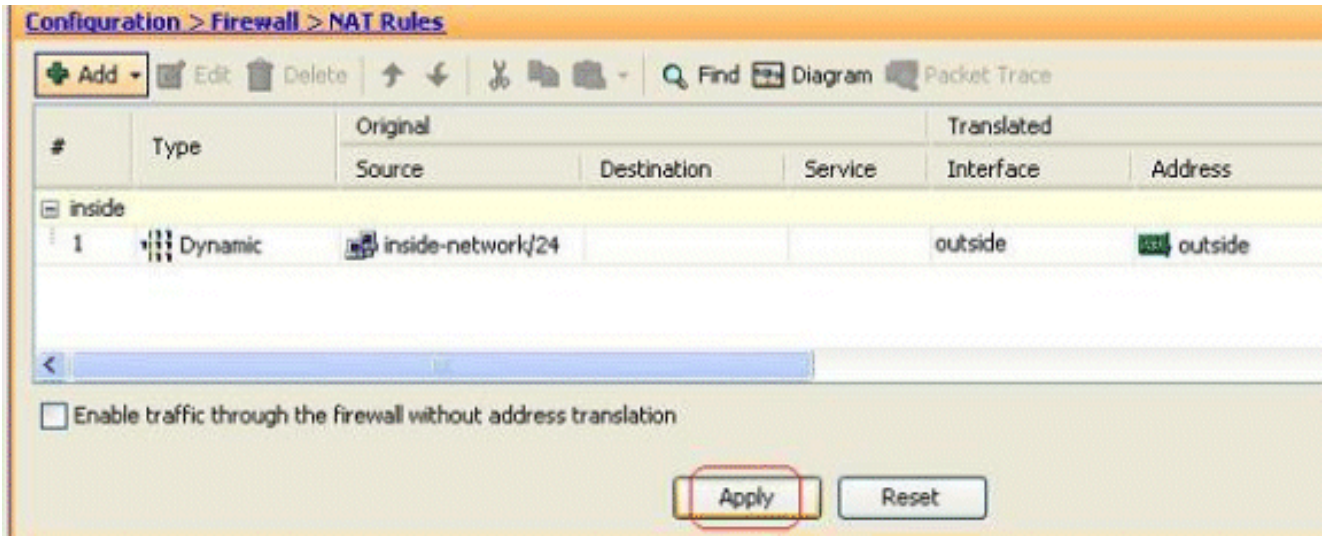
5. Affiché ici est le pool d'adresses configuré avec l'interface extérieure comme seule adresse disponible dans ce groupe. Cliquez sur OK afin de retourner à la fenêtre dynamique de règle NAT d'ajouter.



6. Cliquez sur **OK**.



7. La règle NAT dynamique configurée est affichée ici dans le volet de configuration > de Pare-feu > de règles
   NAT.



C'est le CLI équivalent sorti pour cette configuration PAT :

```
global (outside) 20 interface nat (inside) 20 172.16.11.0 255.255.255.0
```

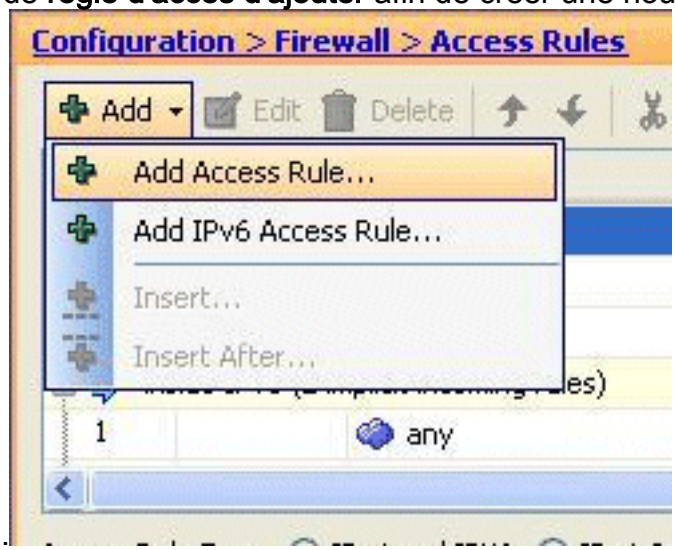
Restreindre l'accès des hôtes internes aux réseaux externes

Quand aucune règle d'accès n'est définie, les utilisateurs d'une interface à sécurité plus élevée peuvent accéder à toutes les ressources associées avec une interface à niveau de sécurité inférieur. Pour limiter certains utilisateurs d'accéder à certaines ressources, règles d'accès d'utilisation dans l'ASDM. Cet exemple décrit comment permettre à un seul utilisateur pour accéder aux ressources extérieures (avec le FTP, le SMTP, le POP3, le HTTPS, et le WWW) et pour limiter tous les autres d'accéder aux ressources extérieures.

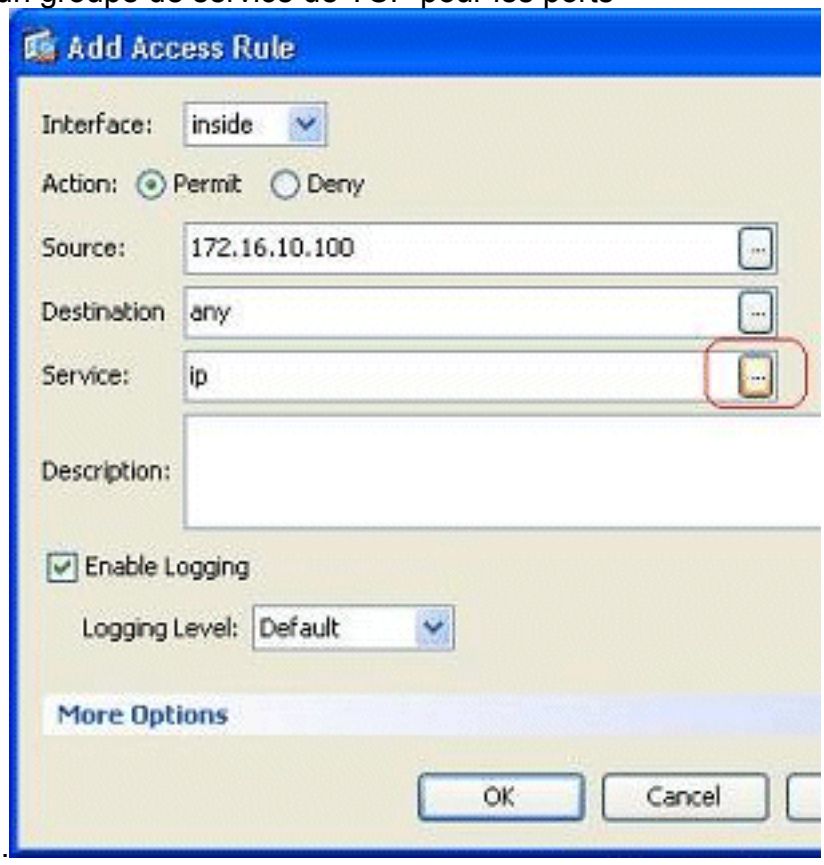
Remarque: Il y aura un « implicite refusent » la règle à la fin de chaque liste d'accès.

Procédez comme suit :

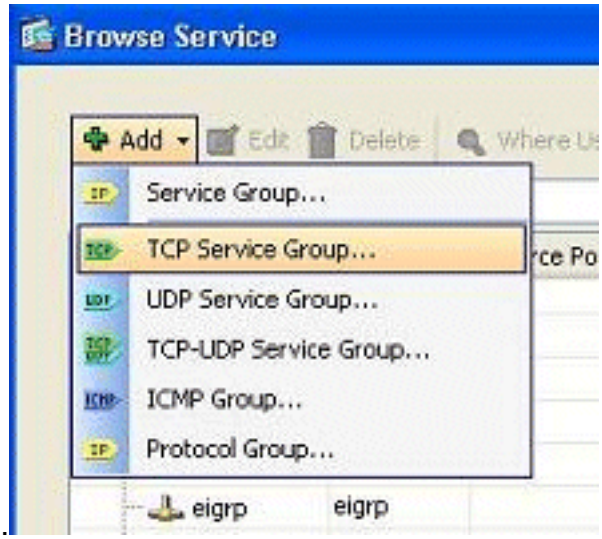
1. Allez à la **configuration** > au **Pare-feu** > aux **règles d'accès**, cliquez sur Add, et choisissez l'option de **règle d'accès d'ajouter** afin de créer une nouvelle entrée de liste d'accès.



2. Choisissez l'adresse IP source qui doit pour être autorisée dans le domaine de **source**. En choisissez comme destination, **à l'intérieur de** comme interface, et **les autorisez** comme action. Pour finir, cliquez sur les **détails** se boutonnent dans le domaine de service afin de créer un groupe de service de TCP pour les ports requis.

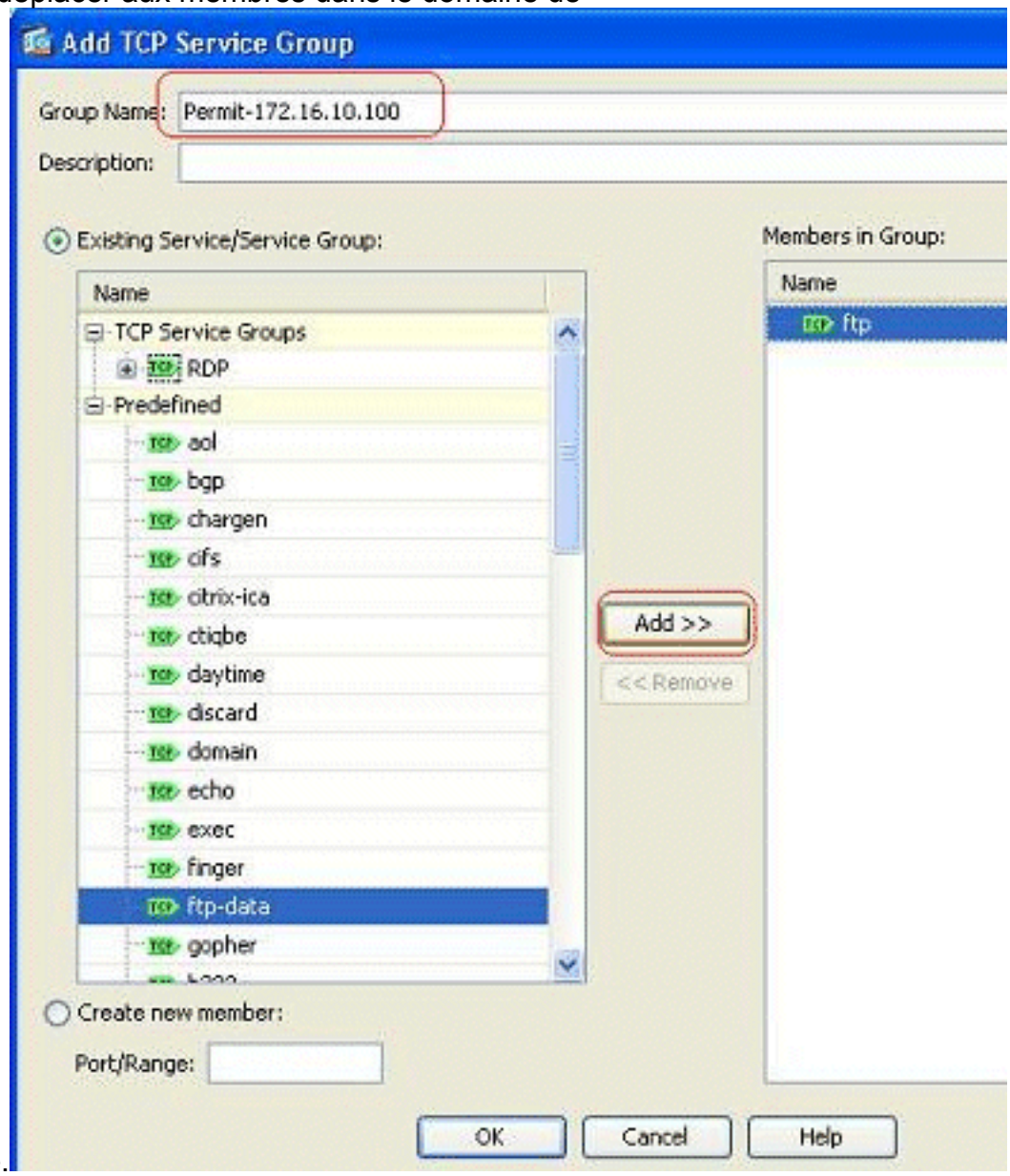


3. Cliquez sur Add, et puis choisissez l'option de **groupe de service de**



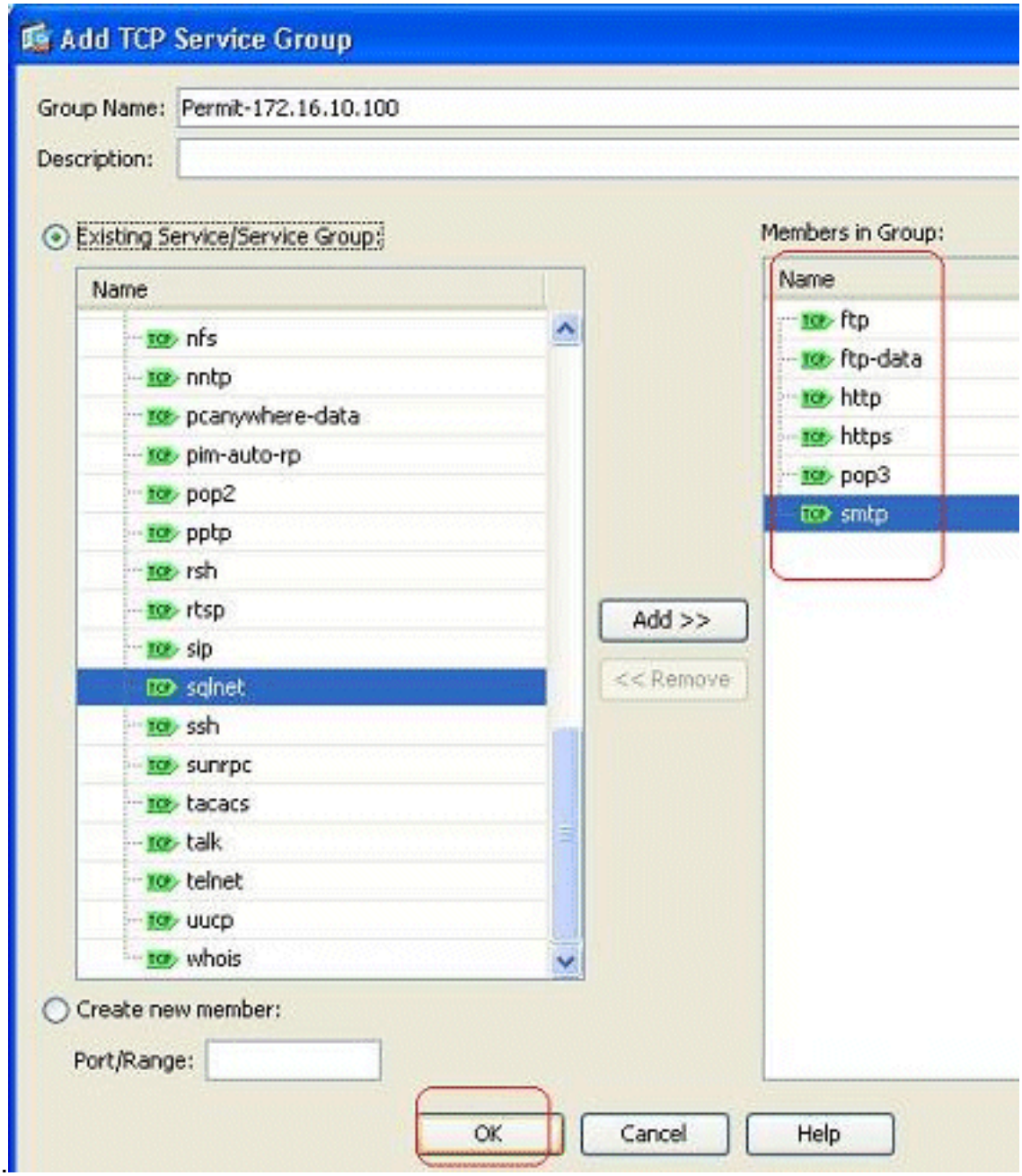
TCP.

4. Écrivez un nom pour ce groupe. Choisissez chacun des ports requis, et cliquez sur Add afin de les déplacer aux membres dans le domaine de



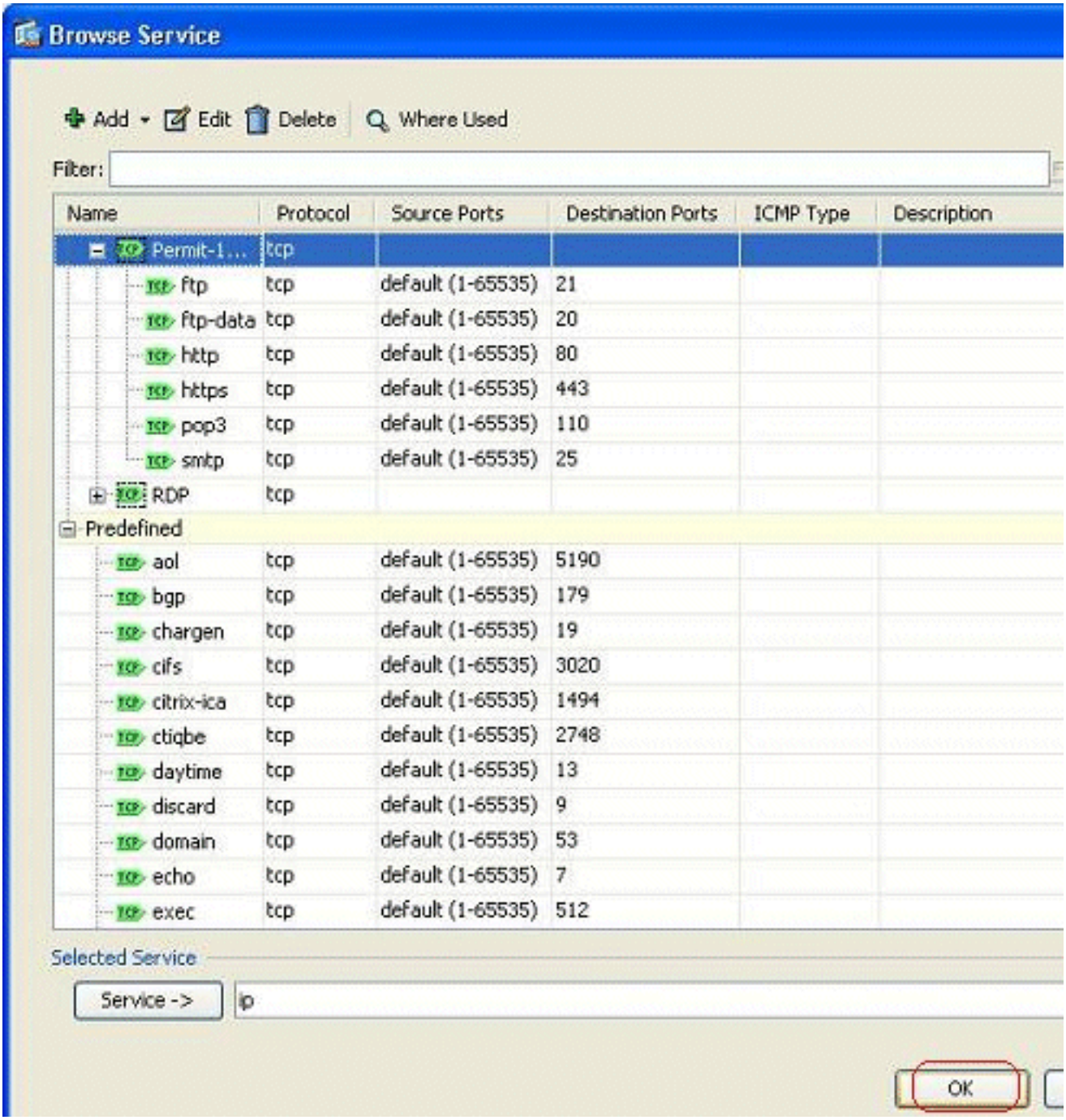
groupe.

5. Vous devriez voir tous les ports sélectionnés dans le domaine droit. Cliquez sur OK afin de se terminer les ports de service sélectionnant le



processus.

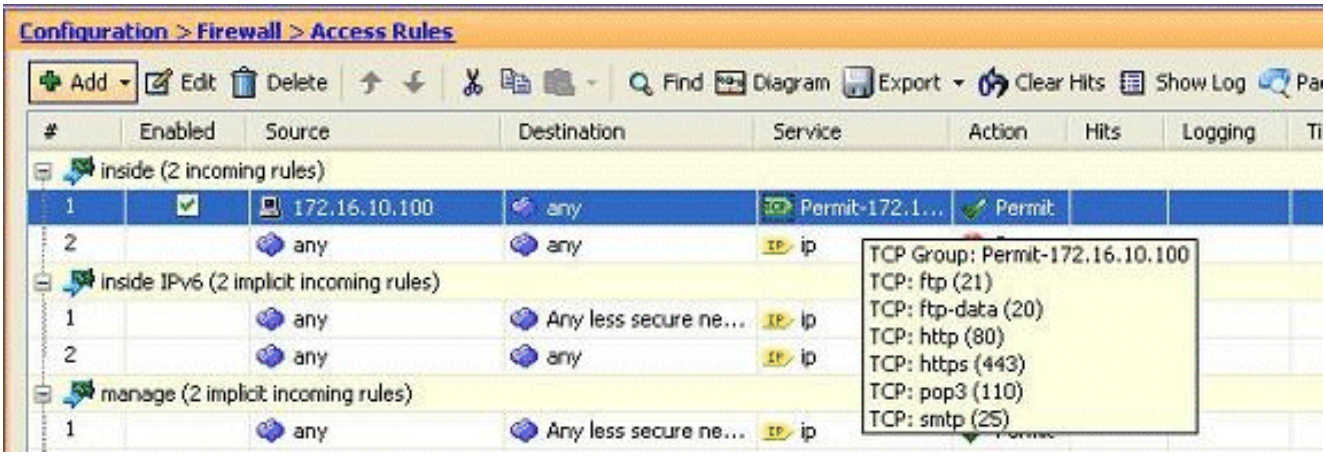
6. Vous pouvez voir le groupe de service configuré de TCP ici. Cliquez sur **OK**.



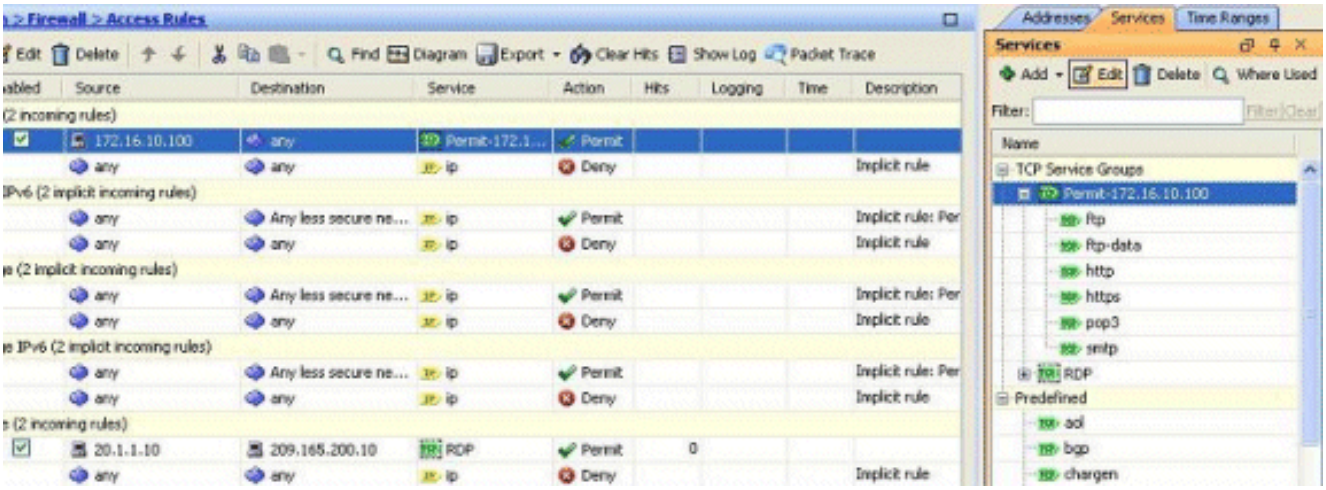
7. Cliquez sur OK afin de se terminer la

configuration.

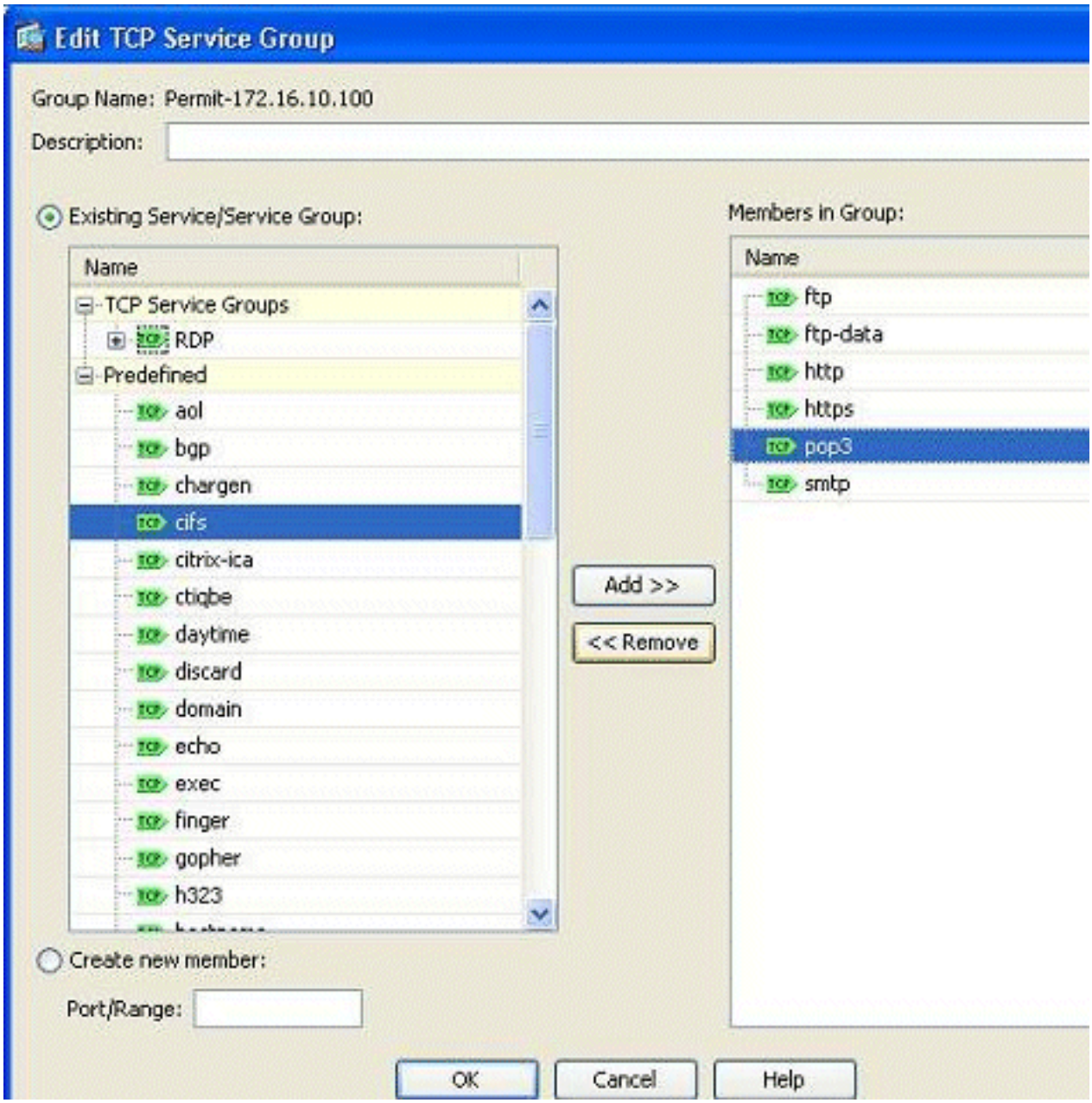
8. La règle d'accès configurée peut être vue sous l'**interface interne** dans le volet de configuration > de Pare-feu > de règles d'accès.



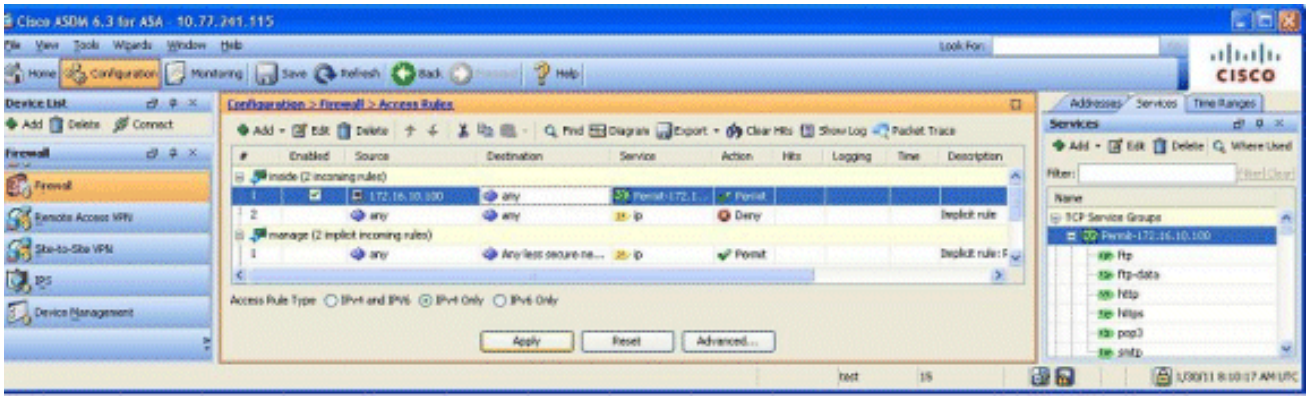
9. Pour la simplicité d'utilisation, vous pourriez également éditer le service-groupe de TCP directement sur le volet droit dans les **services** tableau cliquez sur Edit afin de modifier ce service-groupe directement.



10. Il de nouveau redirect to la fenêtre de groupe de service de TCP d'éditer. Exécutez les modifications basées sur vos conditions requises, et cliquez sur OK afin de sauvegarder les modifications.



11. Affichée ici est une vue complète de l'ASDM
:



C'est la configuration équivalente CLI :

```
object-group service Permit-172.16.10.100 TCP port-object eq ftp port-object eq ftp-data port-object eq www port-object eq https port-object eq pop3 port-object eq smtp ! access-list inside_access_in extended permit TCP host 172.16.10.100 any object-group Permit-172.16.10.100 ! access-group inside_access_in in interface inside !
```

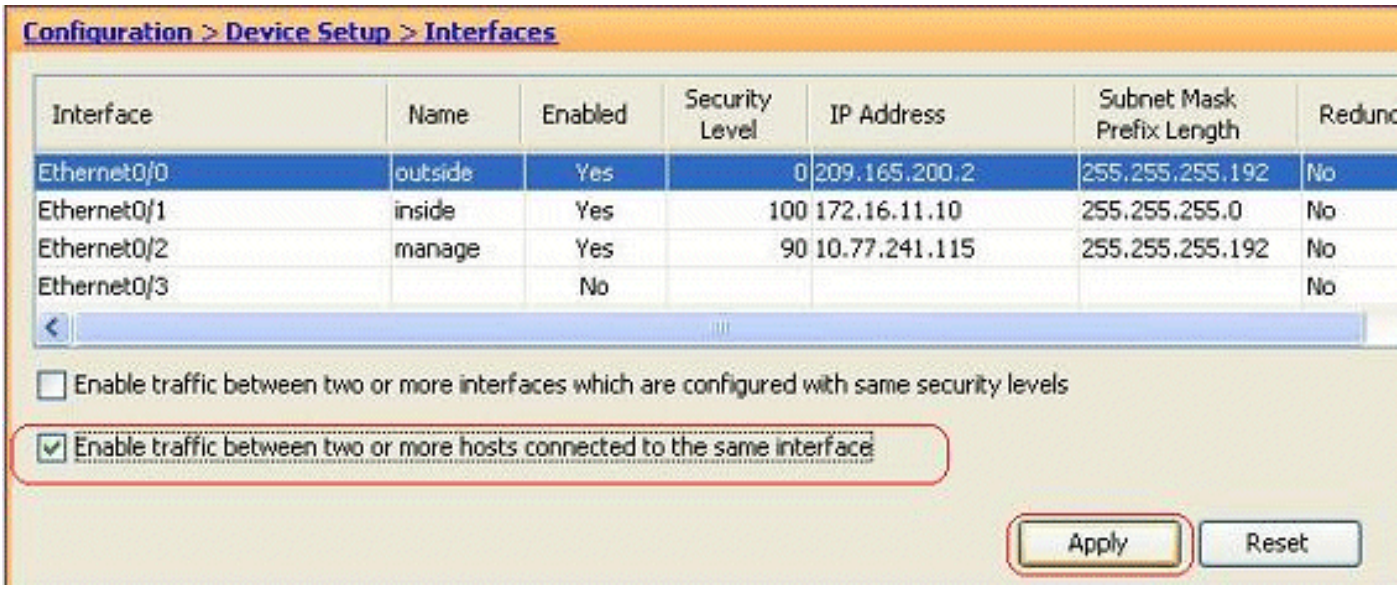
Pour des informations complètes sur mettre en application le contrôle d'accès, référez-vous ajoutent ou modifient une liste d'accès par le GUI ASDM.

Permettez le trafic entre les interfaces avec le même niveau de Sécurité

Cette section décrit comment activer le trafic dans les interfaces qui ont les mêmes niveaux de Sécurité.

Ces instructions décrivent comment activer la transmission intra-interface.

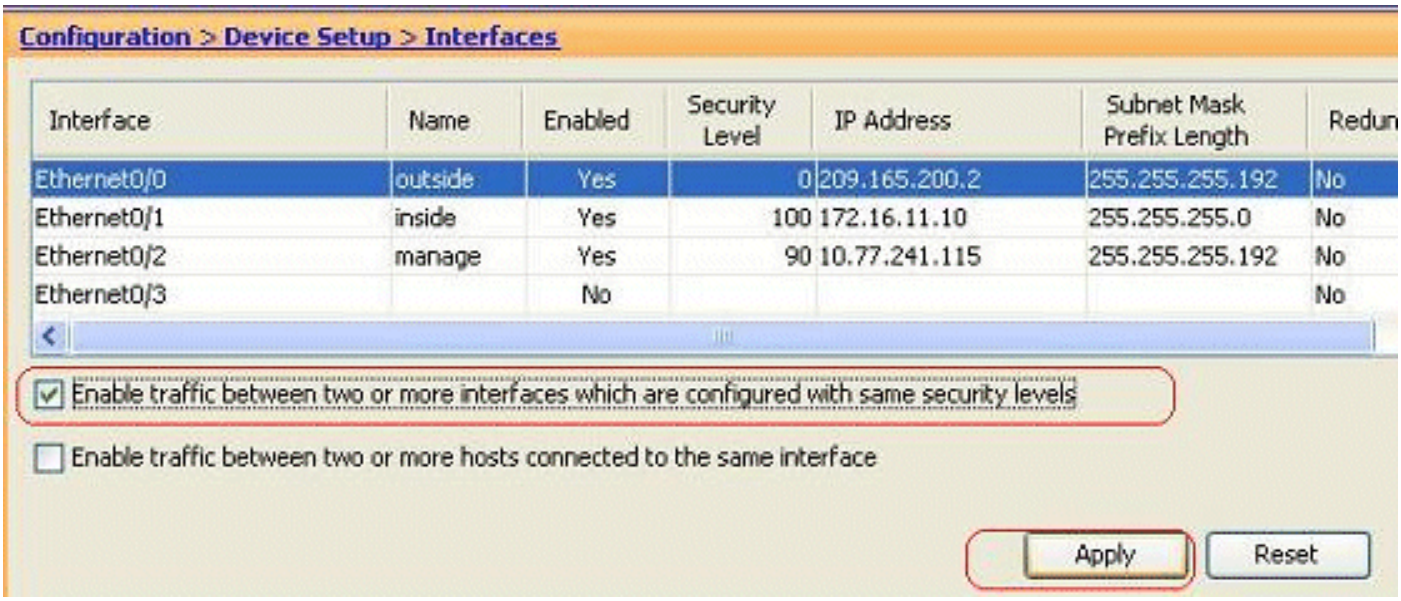
Ce sera utile pour le trafic VPN qui écrit une interface, mais est puis conduit la même interface. Le trafic VPN pourrait être décrypté dans ce cas, ou il pourrait re-être chiffré pour une autre connexion VPN. Allez à la **configuration > installation de périphérique >** des **interfaces**, et choisissent le **trafic d'enable entre deux hôtes ou plus connectés à la même** option d'**interface**.



Ces instructions décrivent comment activer la transmission d'inter-interface.

C'est utile pour permettre la transmission entre les interfaces avec les niveaux de Sécurité égaux.

Allez à la **configuration > installation de périphérique >** des **interfaces**, et choisissent le **trafic d'enable entre deux interfaces ou plus qui sont configurées avec la même** option de **niveaux de Sécurité**.



C'est le CLI équivalent pour chacun des deux configurations :

```
same-security-traffic permit intra-interface
same-security-traffic permit inter-interface
```

Autoriser les hôtes non approuvés à accéder à des hôtes sur votre réseau approuvé

Ceci peut être réalisé en appliquant une traduction NAT statique et une règle d'accès de permettre ces hôtes. Vous exigez de configurer ceci toutes les fois qu'un utilisateur externe voudrait accéder à n'importe quel serveur qui se repose dans votre réseau interne. Le serveur dans le réseau interne aura une adresse IP privée qui n'est pas routable sur l'Internet. En conséquence, vous devez traduire cette adresse IP privée à une adresse IP publique par une règle NAT statique. Supposez que vous avez un serveur interne (172.16.11.5). Afin de faire ce travail, vous devez traduire cet IP privé de serveur à un IP de public. Cet exemple décrit comment implémenter le NAT statique bidirectionnel pour traduire 172.16.11.5 à 209.165.200.5.

La section sur permettre à l'utilisateur externe pour accéder à ce web server en mettant en application une règle d'accès n'est pas affichée ici. Un extrait CLI de brief est affiché ici pour votre compréhension :

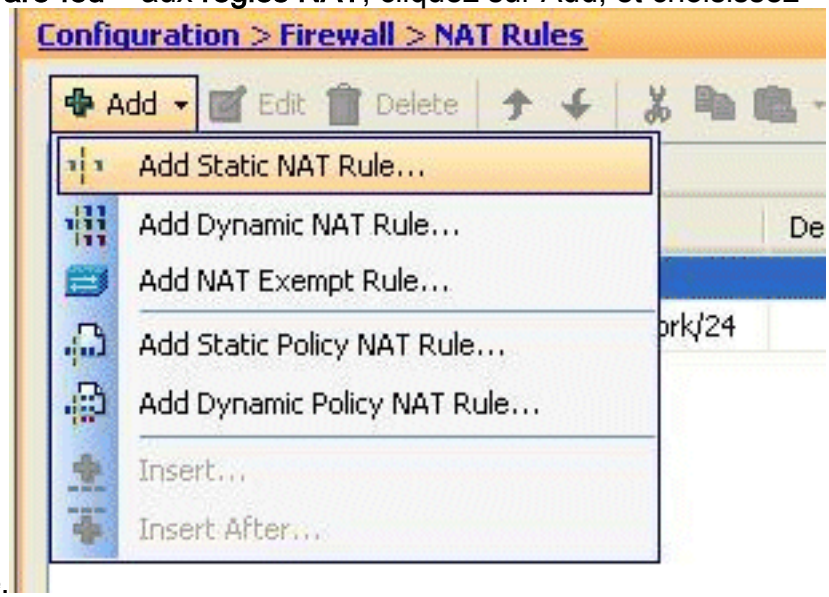
```
access-list 101 permit TCP any host 209.165.200.5
```

Le pour en savoir plus, se rapportent ajoutent ou modifient une liste d'accès par le GUI ASDM.

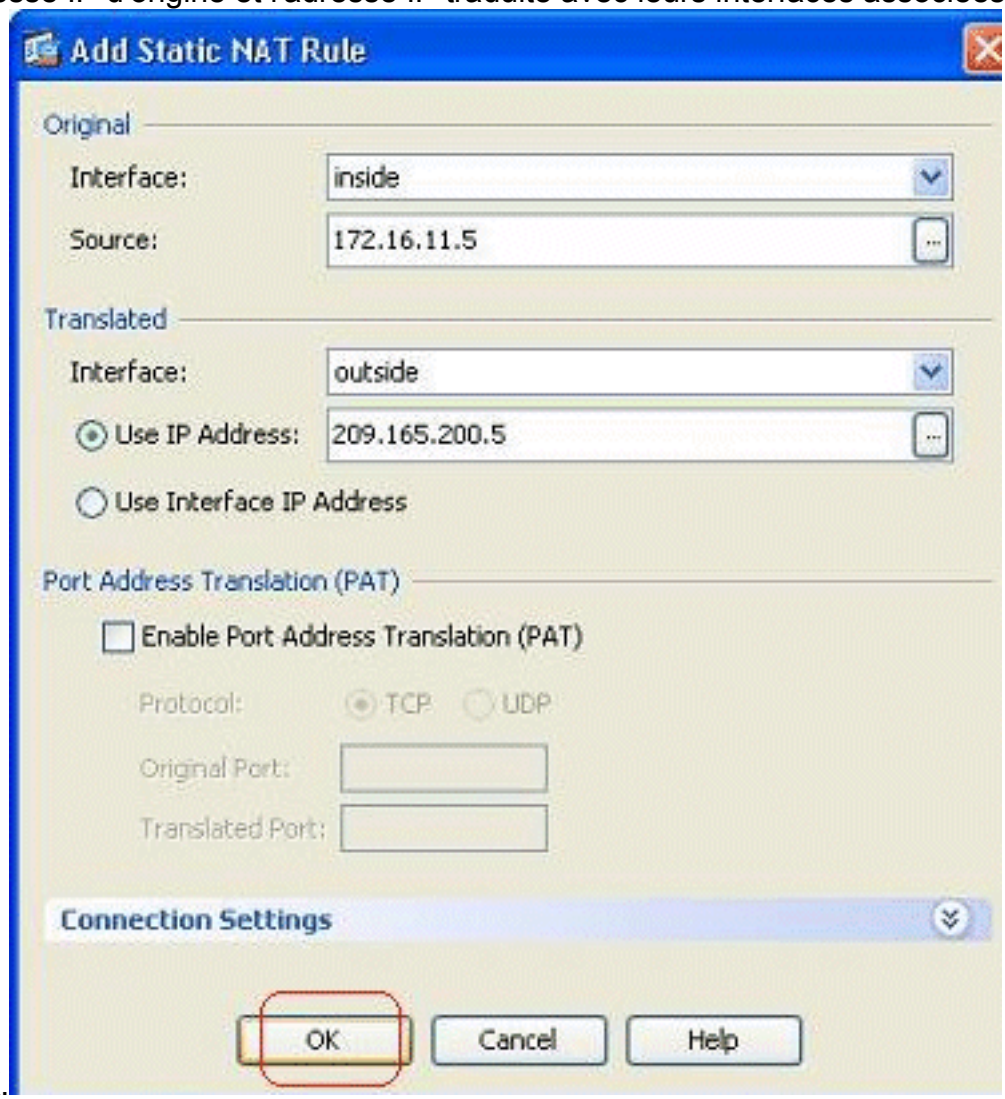
Remarque: Spécifier le mot clé « » permet à n'importe quel utilisateur du monde extérieur pour accéder à ce serveur. En outre, s'il n'est spécifié pour aucun port de service, le serveur peut être accédé à sur n'importe quel port de service pendant que ces séjour ouvert. Précaution d'usage quand vous mise en place, et vous êtes informé limiter l'autorisation à l'utilisateur externe individuel et également au port prié sur le serveur.

Terminez-vous ces étapes afin de configurer le NAT statique :

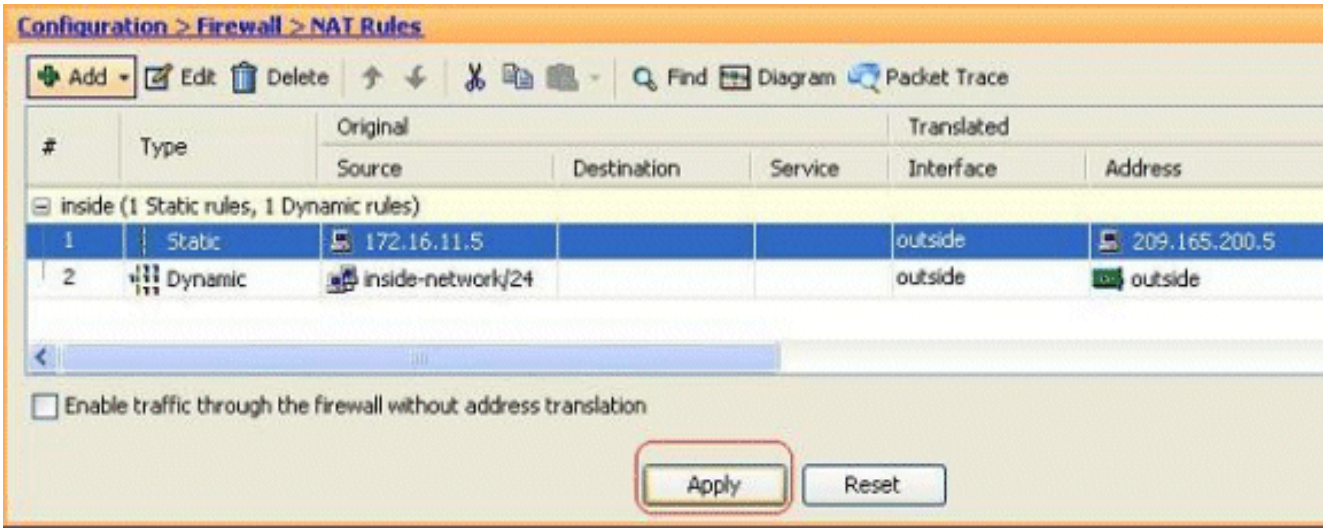
1. Allez à la **configuration** > au **Pare-feu** > aux **règles NAT**, cliquez sur Add, et choisissez **ajoutent la règle NAT statique**.



2. Spécifiez l'adresse IP d'origine et l'adresse IP traduite avec leurs interfaces associées, et cliquez sur OK.



3. Vous pouvez voir l'entrée NAT statique configurée ici. Cliquez sur Apply afin d'envoyer ceci à l'ASA.



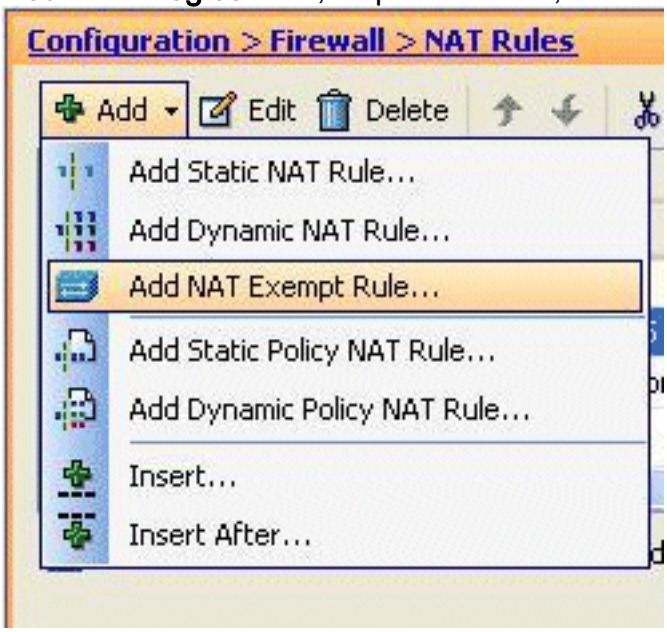
C'est un exemple CLI de brief pour cette configuration ASDM :

```
! static (inside,outside) 209.165.200.5 172.16.11.5 netmask 255.255.255.255 !
```

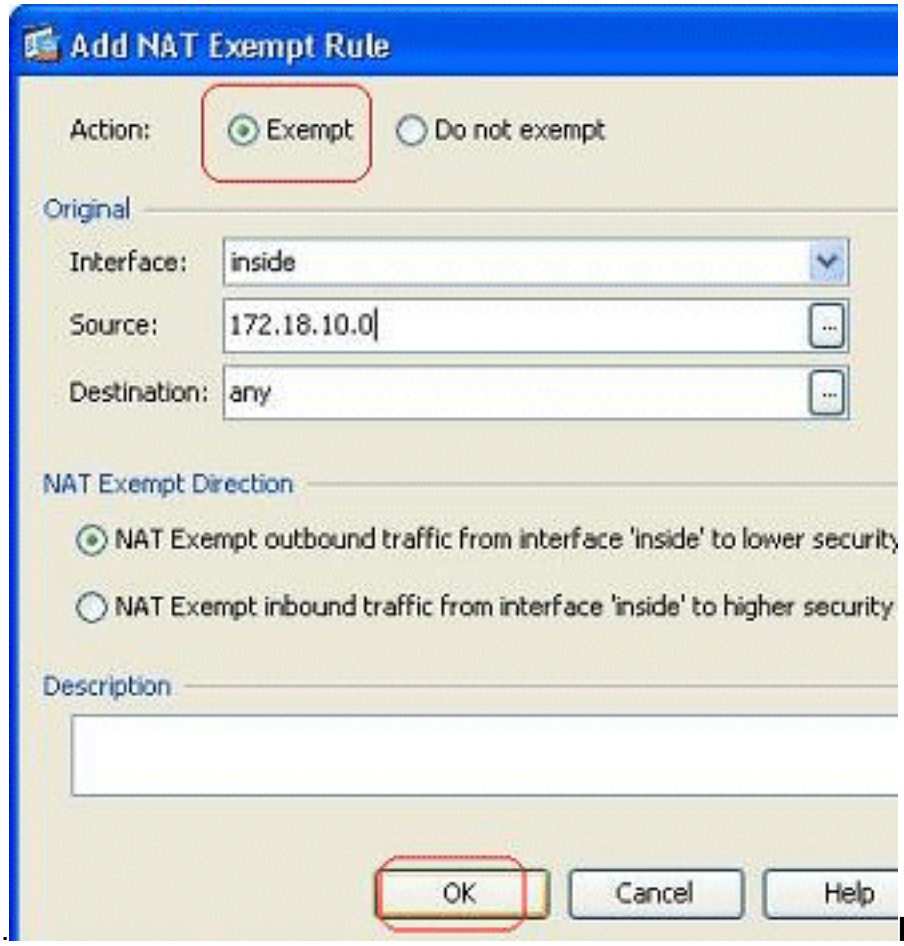
Désactiver NAT pour des hôtes/réseaux spécifiques

Quand vous devez exempter des hôtes spécifiques ou des réseaux de NAT, ajoutez un NAT exemptent la règle de désactiver la traduction d'adresses. Ceci laisse traduit et des serveurs distants pour initier des connexions.

Procédez comme suit :

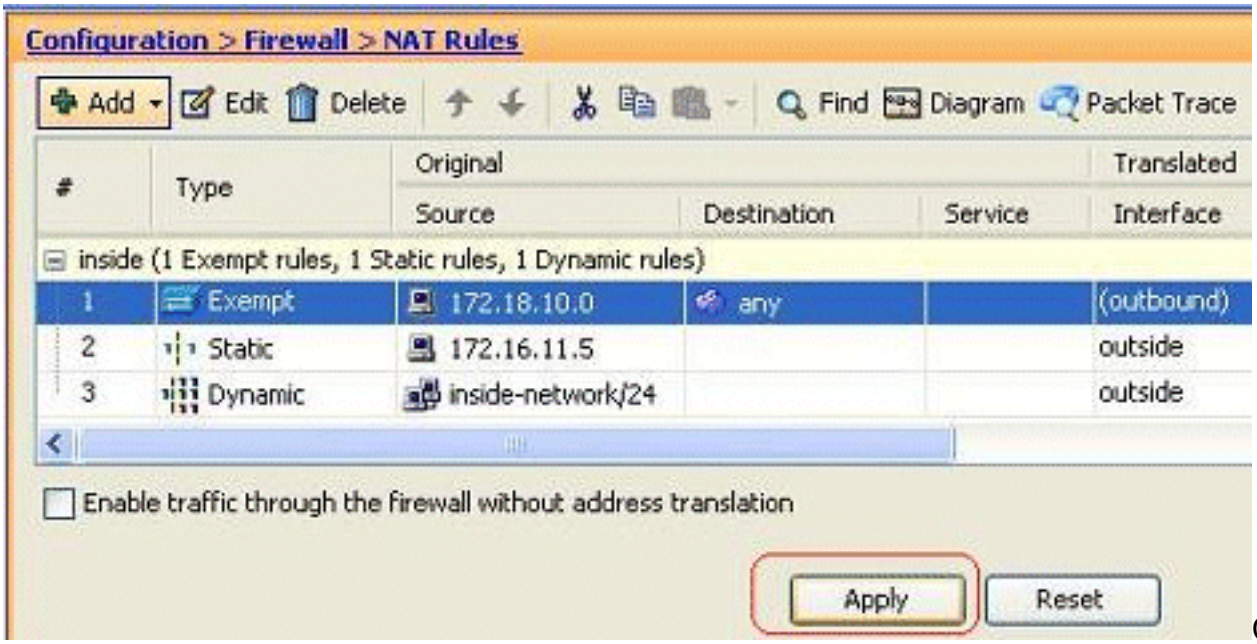
1. Allez à la **configuration** > au **Pare-feu** > aux **règles NAT**, cliquez sur Add, et choisissez **ajoutent NAT exemptent la règle**.


2. Ici, le réseau intérieur 172.18.10.0 a été exempté de la traduction d'adresses. Assurez-vous que l'option **exempte** a été sélectionnée. La direction exempte NAT a deux options :Le trafic sortant aux interfaces à niveau de sécurité inférieurLe trafic d'arrivée aux interfaces à sécurité plus élevéeL'option par défaut est pour le trafic sortant. Cliquez sur OK afin de se terminer



l'étape. **Remarque:** Quand vous choisissez **n'exemptez pas l'**option, cet hôte spécifique ne sera pas exempté de NAT et une règle d'accès distincte sera ajoutée avec « refusent » le mot clé. C'est utile en évitant des hôtes spécifiques de toutexempt NAT que le sous-réseau complet, à l'exclusion de ces hôtes, sera NAT exempté.

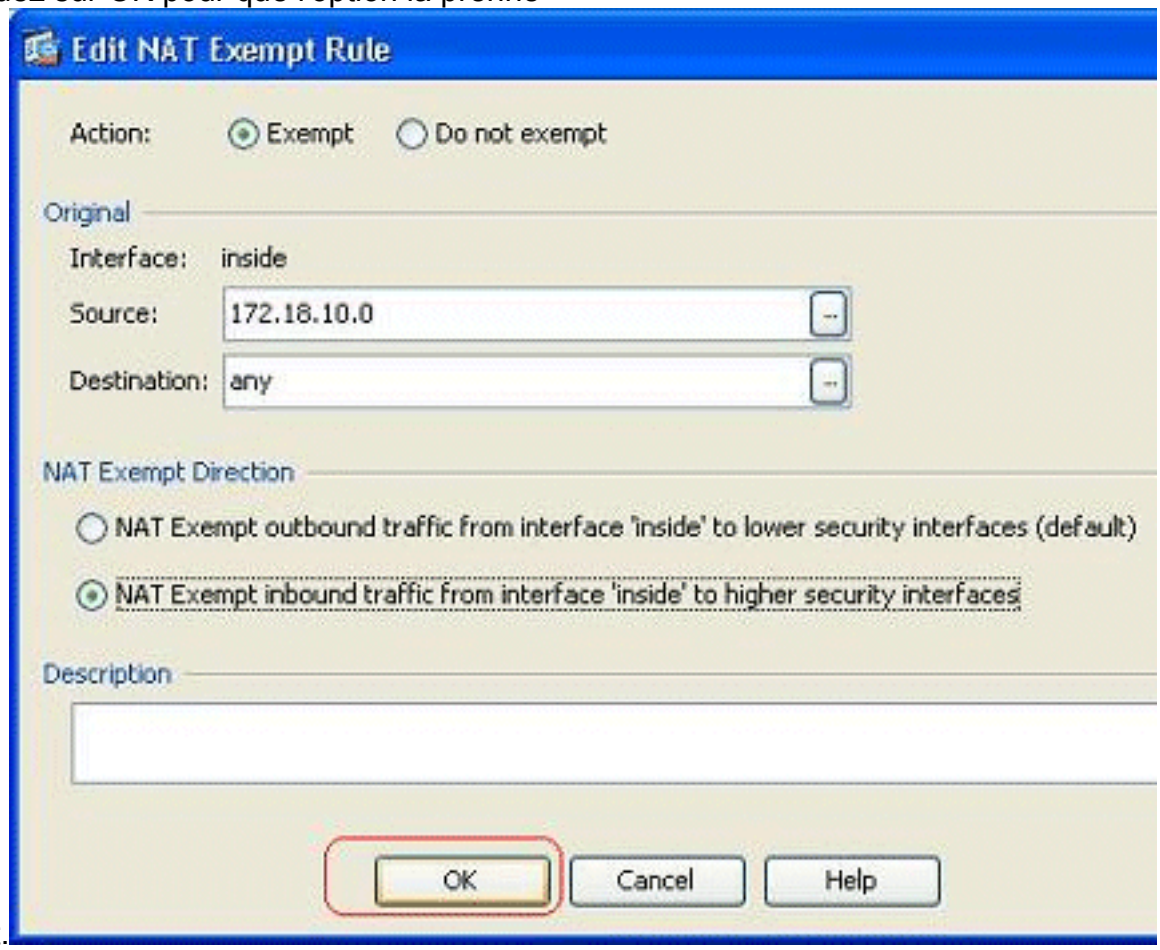
3. Vous pouvez voir le NAT exempter la règle pour la direction sortante ici. Cliquez sur Apply afin d'envoyer la configuration à l'ASA.



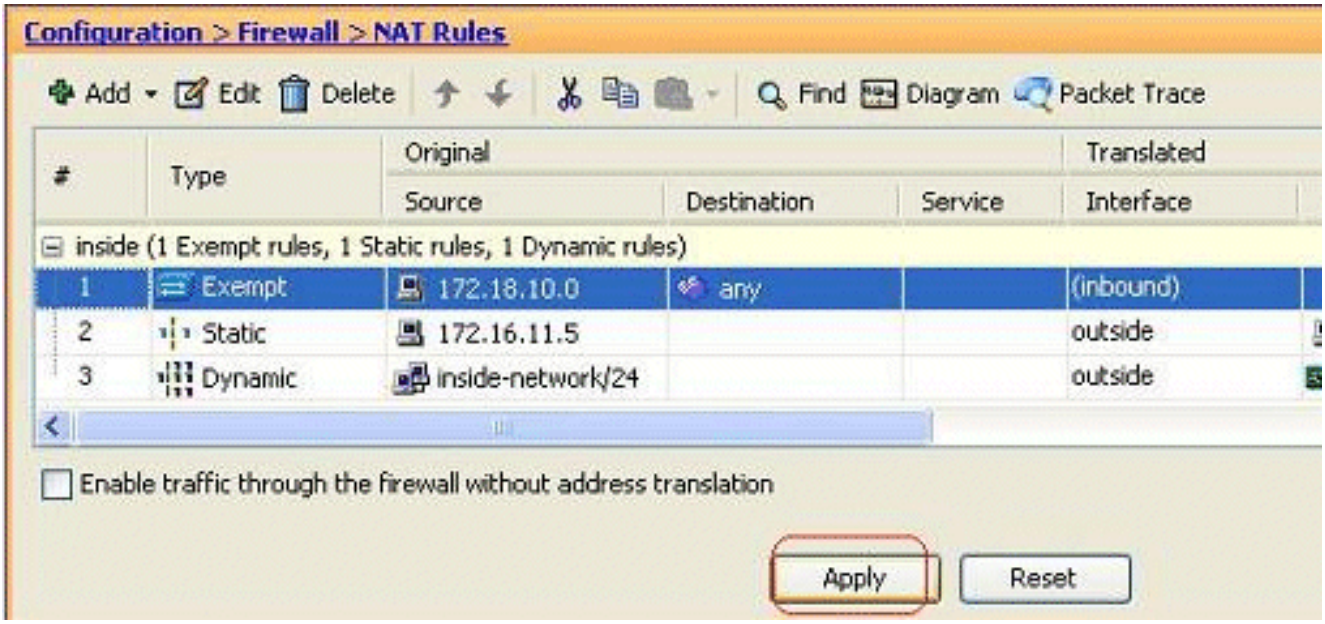
C'est la sortie équivalente CLI pour votre référence :

```
access-list inside_nat0_outbound extended
permit ip host 172.18.10.0 any
!
nat (inside) 0 access-list inside_nat0_outbound
```

4. Voici que vous pouvez voir comment éditer le NAT exemptez la règle pour sa direction. Cliquez sur OK pour que l'option la prenne effet.



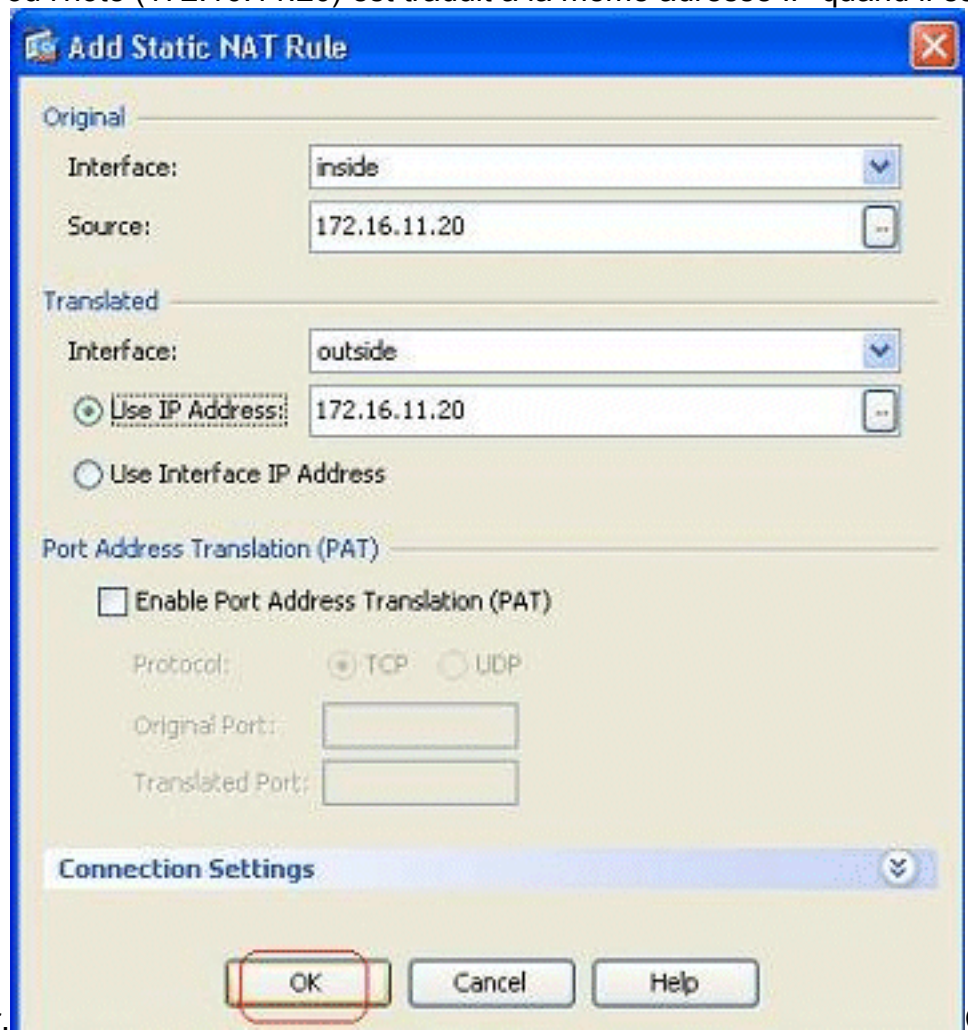
5. Vous pouvez maintenant voir que la direction a été changée à *d'arrivée*.



Cliquez sur Apply afin d'envoyer ce CLI sorti à l'ASA :`access-list inside_nat0_outbound extended permit ip host 172.18.10.0 any`
`!`
`nat (inside) 0 access-list inside_nat0_outbound` **`outside`** **Remarque:** De ceci, vous pouvez voir qu'un nouveau mot clé (dehors) a été ajouté pour finir des **0** commandes **nat**. Cette caractéristique s'appelle un **extérieur NAT**.

6. Une autre manière de désactiver NAT est par l'implémentation de l'identité NAT. L'identité

NAT traduit un hôte à la même adresse IP. Voici un exemple NAT d'identité statique régulière, où l'hôte (172.16.11.20) est traduit à la même adresse IP quand il est accédé à de



l'extérieur. C'est le CLI équivalent sorti :

```
! static (inside,outside) 172.16.11.20 172.16.11.20 netmask 255.255.255.255 !
```

Port Redirection(Forwarding) avec des commandes static

La transmission du port ou la redirection de port est une fonctionnalité utile où l'essai d'utilisateurs externes accéder à un serveur interne sur un port spécifique. Afin de réaliser ceci, le serveur interne, qui a une adresse IP privée, sera traduit à une adresse IP publique qui consécutivement est permis l'accès pour le port spécifique.

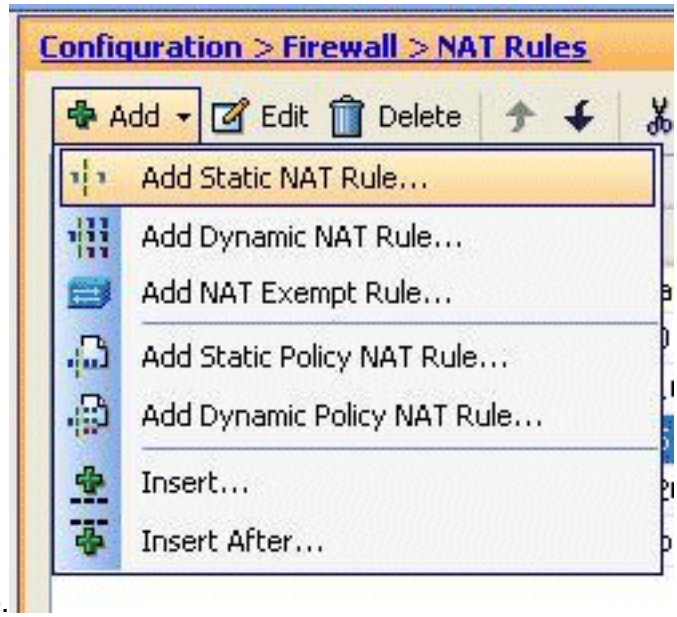
Dans cet exemple, l'utilisateur externe veut accéder au serveur SMTP, 209.165.200.15 au port 25. Ceci est accompli dans deux étapes :

1. Traduisez le serveur de messagerie interne, 172.16.11.15 sur le port 25, à l'adresse IP publique, 209.165.200.15 au port 25.
2. Permettez l'accès au serveur de messagerie public, 209.165.200.15 au port 25.

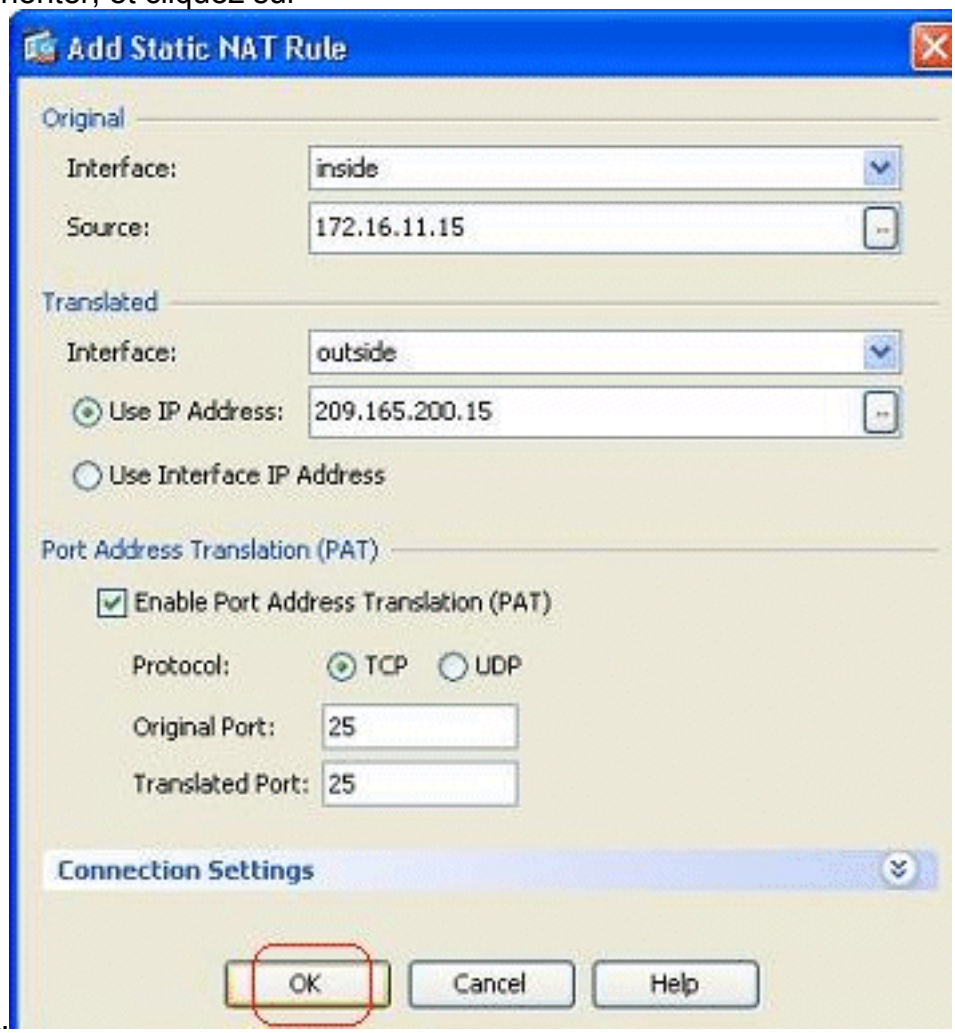
Quand les essais d'utilisateur externe pour accéder au serveur, 209.165.200.15 au port 25, ce trafic seront réorientés au serveur de messagerie interne, 172.16.11 15 au port 25.

1. Allez à la **configuration** > au **Pare-feu** > aux **règles NAT**, cliquez sur Add, et choisissez

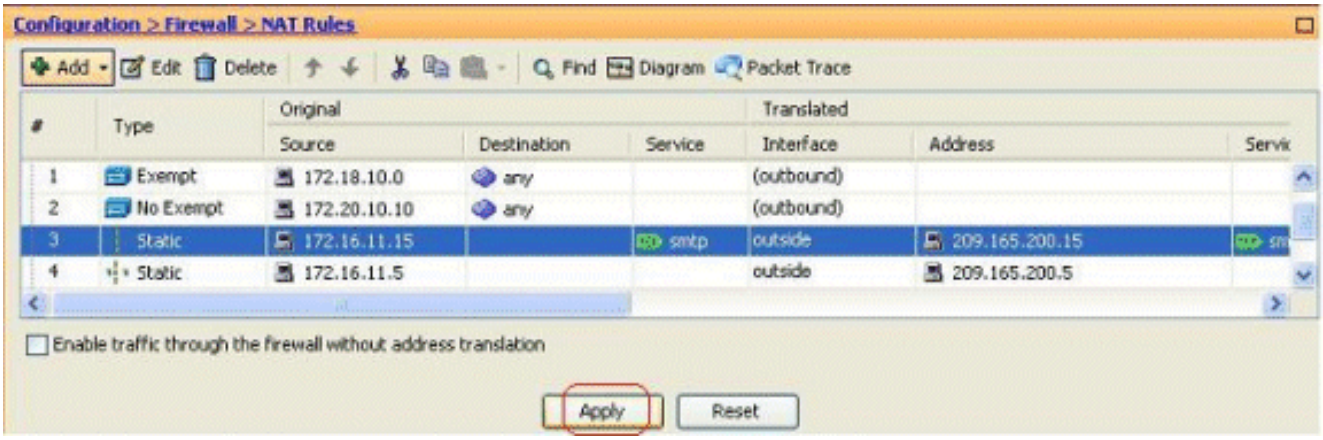
ajoutent la règle NAT statique.



2. Spécifiez la source d'origine et l'adresse IP traduite avec leurs interfaces associées. Choisissez Enable la **translation d'adresses d'adresse du port (PAT)**, spécifiez les ports à réorienter, et cliquez sur OK.



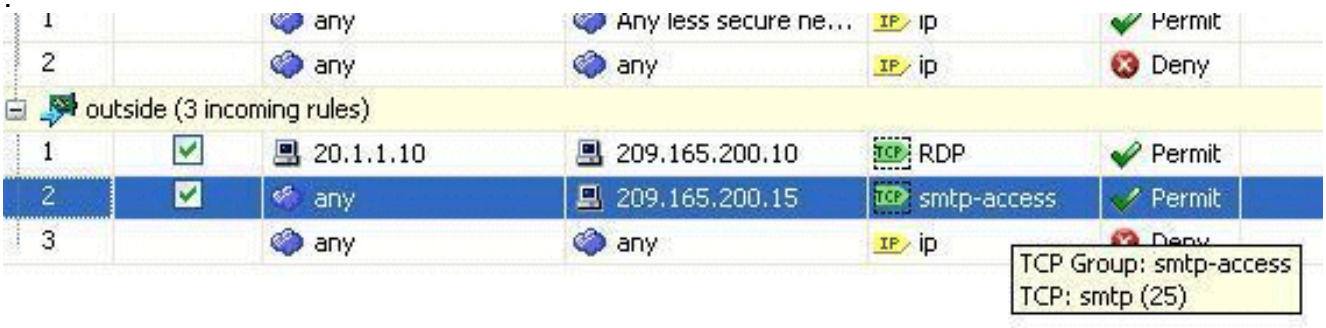
3. La règle configurée de PAT statique est vue ici :



C'est le CLI équivalent sorti :

```
! static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask 255.255.255.255
!
```

4. C'est la règle d'accès qui permet à l'utilisateur externe pour accéder au serveur public de SMTP chez 209.165.200.15
:



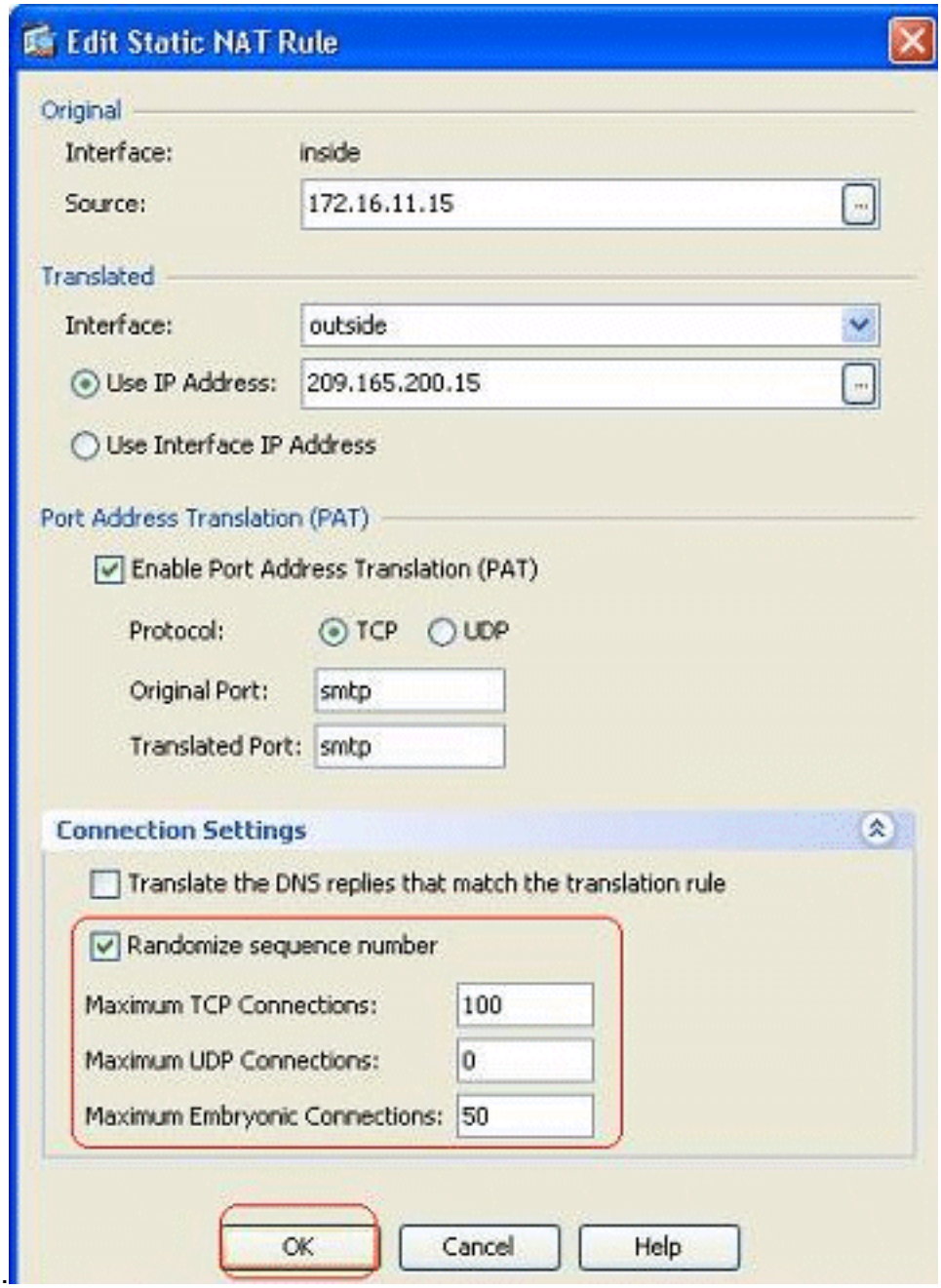
Remarque: Veillez à utiliser des hôtes spécifiques au lieu d'utiliser le **n'importe quel** mot clé dans la source de règle d'accès.

Limiter une session TCP/UDP à l'aide de la commande static

Vous pouvez spécifier le nombre maximal de connexions TCP/UDP à l'aide de la règle statique. Vous pouvez également spécifier le nombre maximal de connexions embryonnaires. Une connexion embryonnaire est une connexion qui est un état entrouvert. Un plus grand nombre de ces derniers affectera la représentation de l'ASA. La limitation de ces connexions empêchera certaines attaques comme le DOS et la synchronisation dans une certaine mesure. Pour la réduction complète, vous devez définir la stratégie dans le cadre MPF, qui est hors de portée de ce document. Pour des informations supplémentaires sur ce thème, référez-vous à atténuer les attaques réseau.

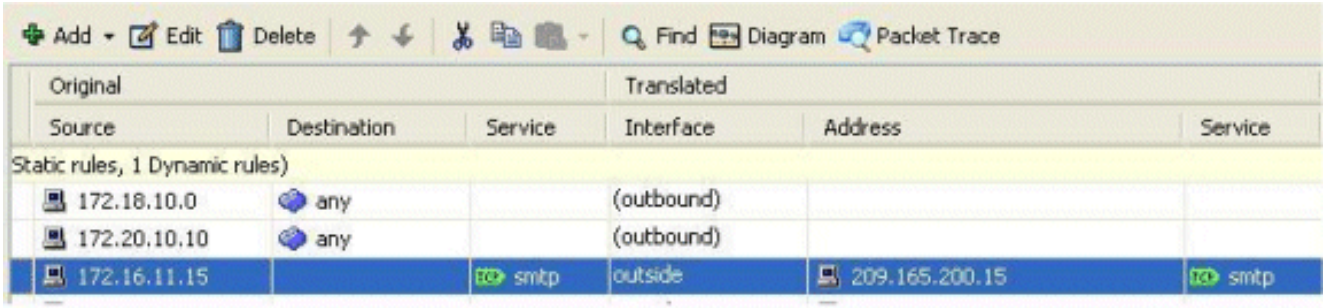
Procédez comme suit :

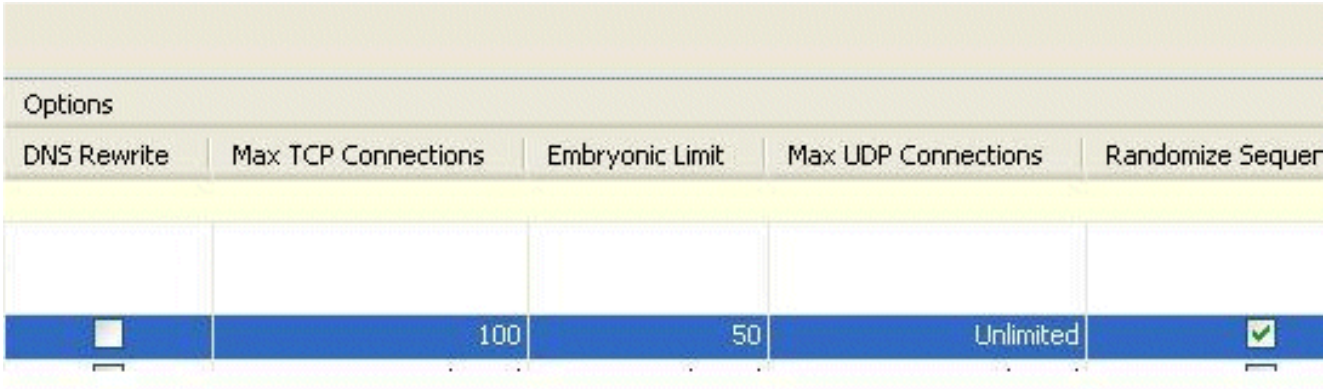
1. Cliquez sur l'onglet de **paramètres de connexion**, et spécifiez les valeurs pour les nombres maximaux de connexions pour cette traduction



statique.

2. Ces images affichent les limites de connexion pour cette traduction statique spécifique :





C'est le CLI équivalent sorti :!

```
static (inside,outside) TCP 209.165.200.15 smtp 172.16.11.15 smtp netmask 255.255.255.255
TCP 100 50 !
```

Liste d'accès basée sur le temps

Cette section traite mettre en application les Listes d'accès basées sur temps à l'aide de l'ASDM. Les règles d'accès peuvent être appliquées basées sur le temps. Afin d'implémenter ceci, vous devez définir une time-range qui spécifie les synchronisations par jour/semaine/mois/année. Puis, vous devez lier cette time-range à la règle d'accès priée. La time-range peut être définie de deux manières :

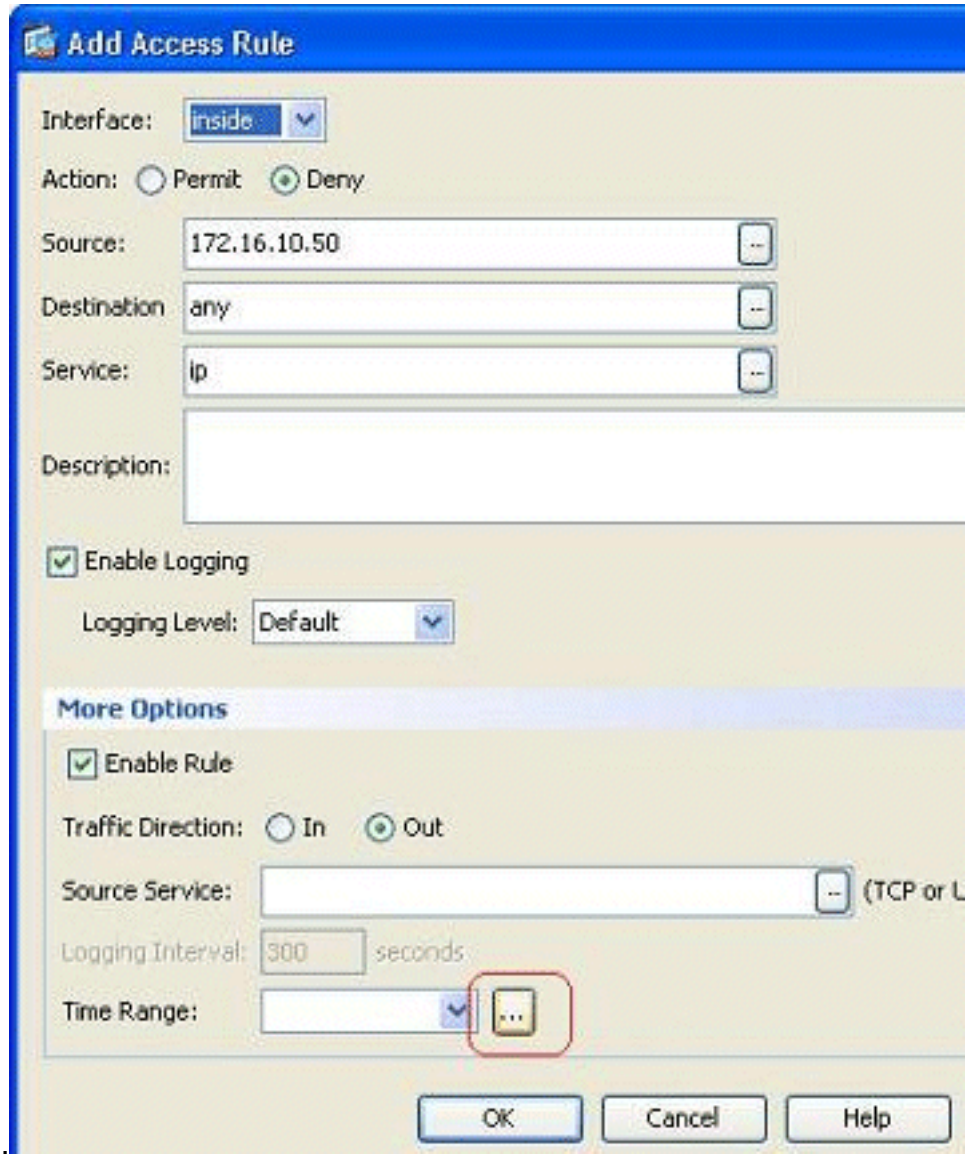
1. Absolu - Définit un délai prévu avec commencer le temps et l'heure de fin.
2. Périodique - Également connu en tant que reproduction. Définit un délai prévu qui se produit aux intervalles spécifiés.

Remarque: Avant que vous configuriez la time-range, assurez-vous que l'ASA a été configurée avec les configurations correctes de date/heure pendant que cette caractéristique emploie les configurations d'horloge système pour implémenter. Avoir l'ASA synchronisée avec le serveur de NTP donnera des résultats bien meilleurs.

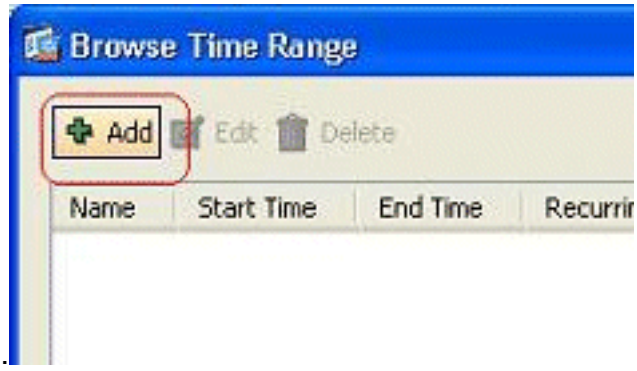
Terminez-vous ces étapes afin de configurer cette caractéristique par l'ASDM :

1. Tout en définissant la règle d'accès, cliquez sur les **détails** se boutonnent dans le domaine

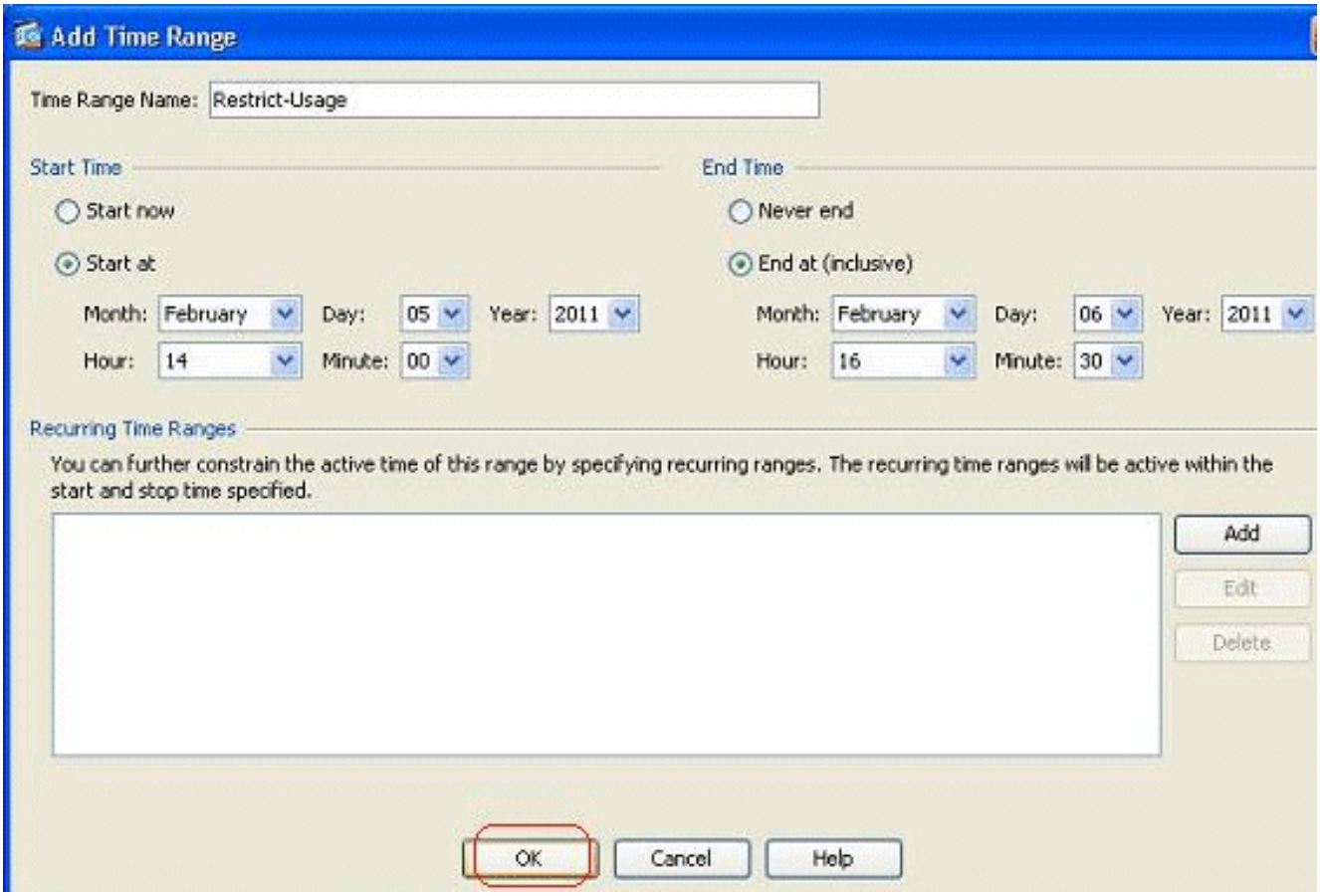
de plage de temps.



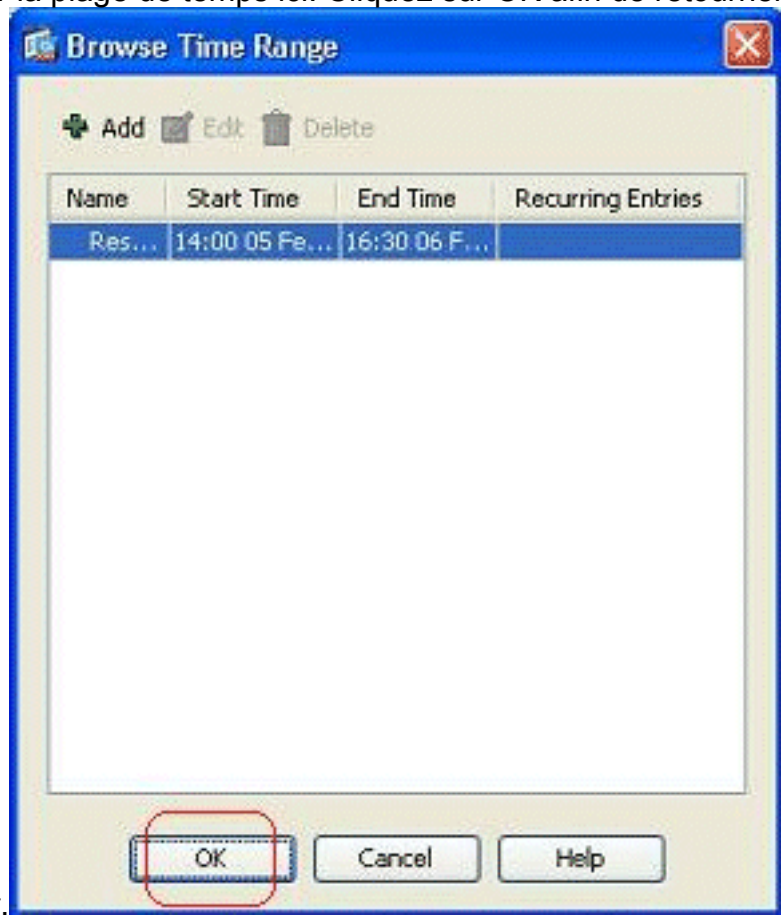
2. Cliquez sur Add afin de créer une nouvelle time-range.



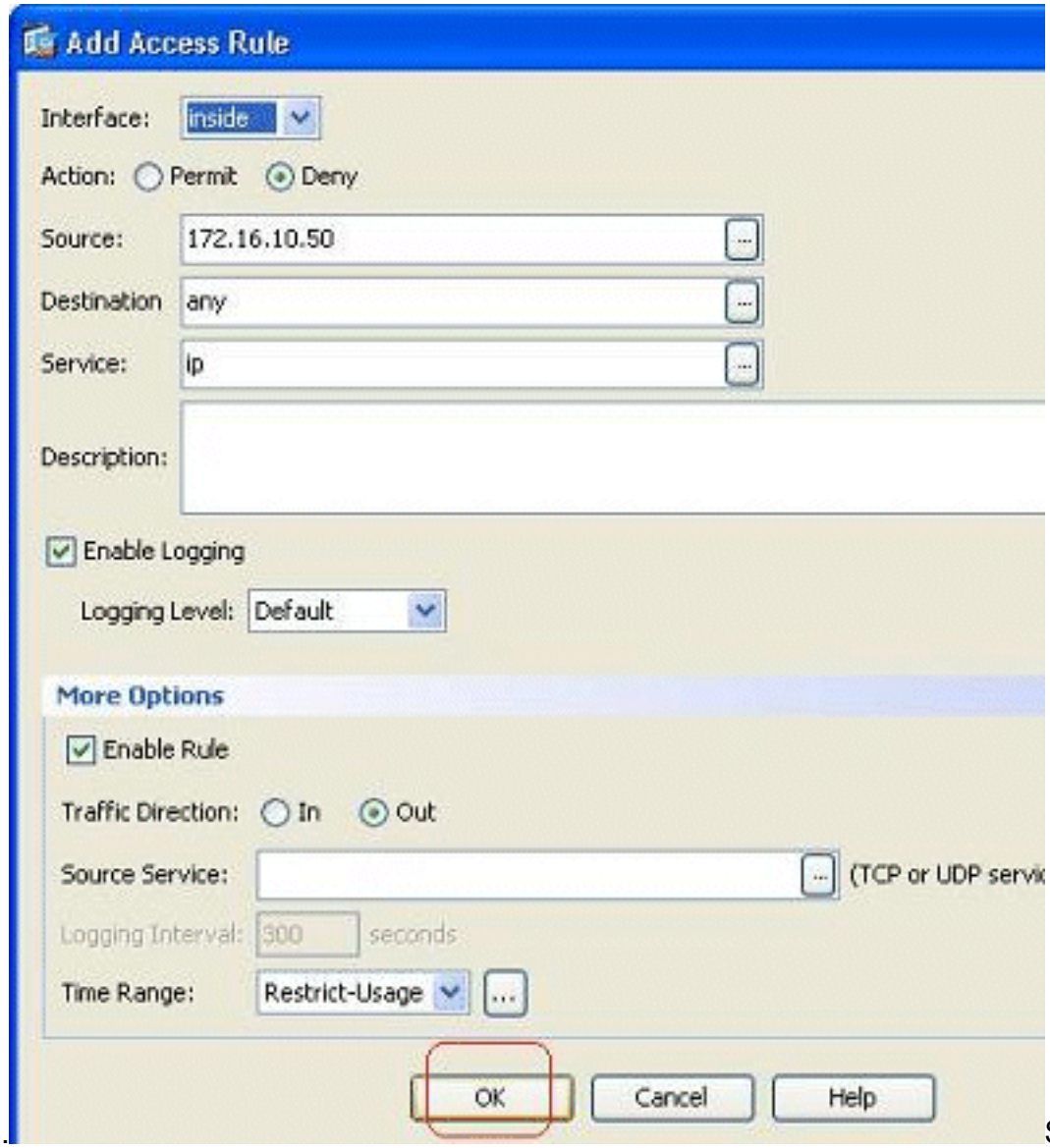
3. Définissez le nom de la plage de temps, et spécifiez le temps et l'heure de fin commençants. Cliquez sur
OK.



4. Vous pouvez voir la plage de temps ici. Cliquez sur OK afin de retourner à la fenêtre de règle d'accès d'ajouter.



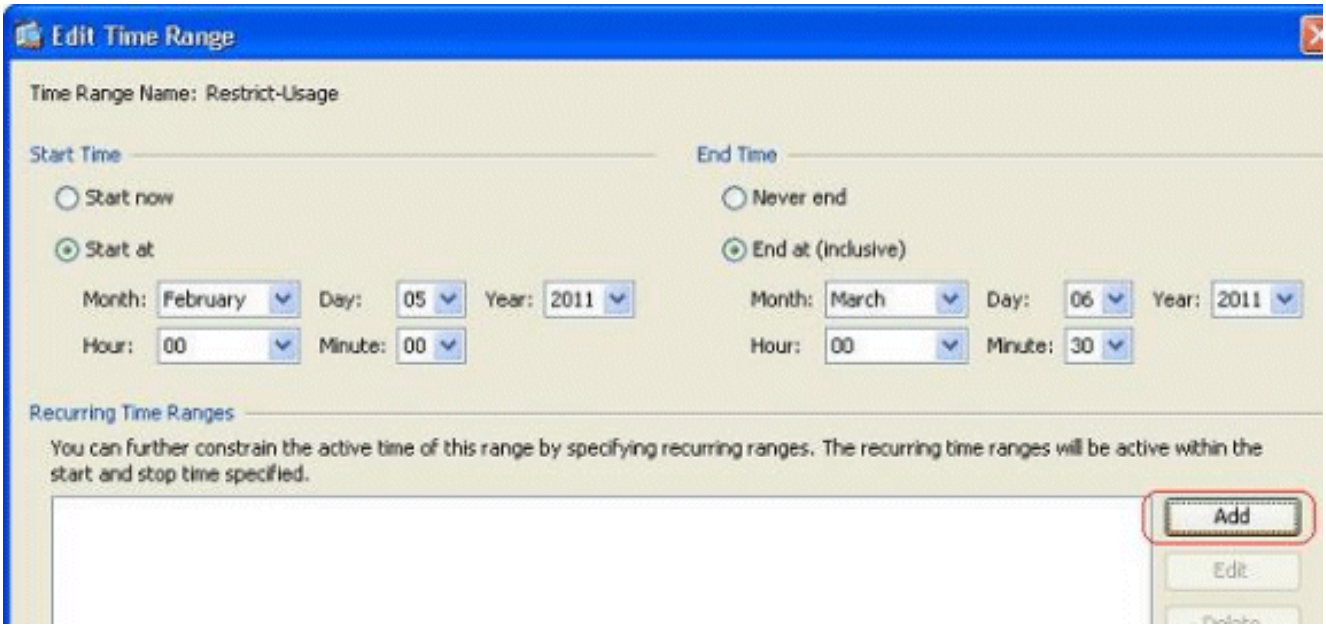
5. Vous pouvez maintenant voir que la plage de temps de Limiter-utilisation a été liée à cette règle



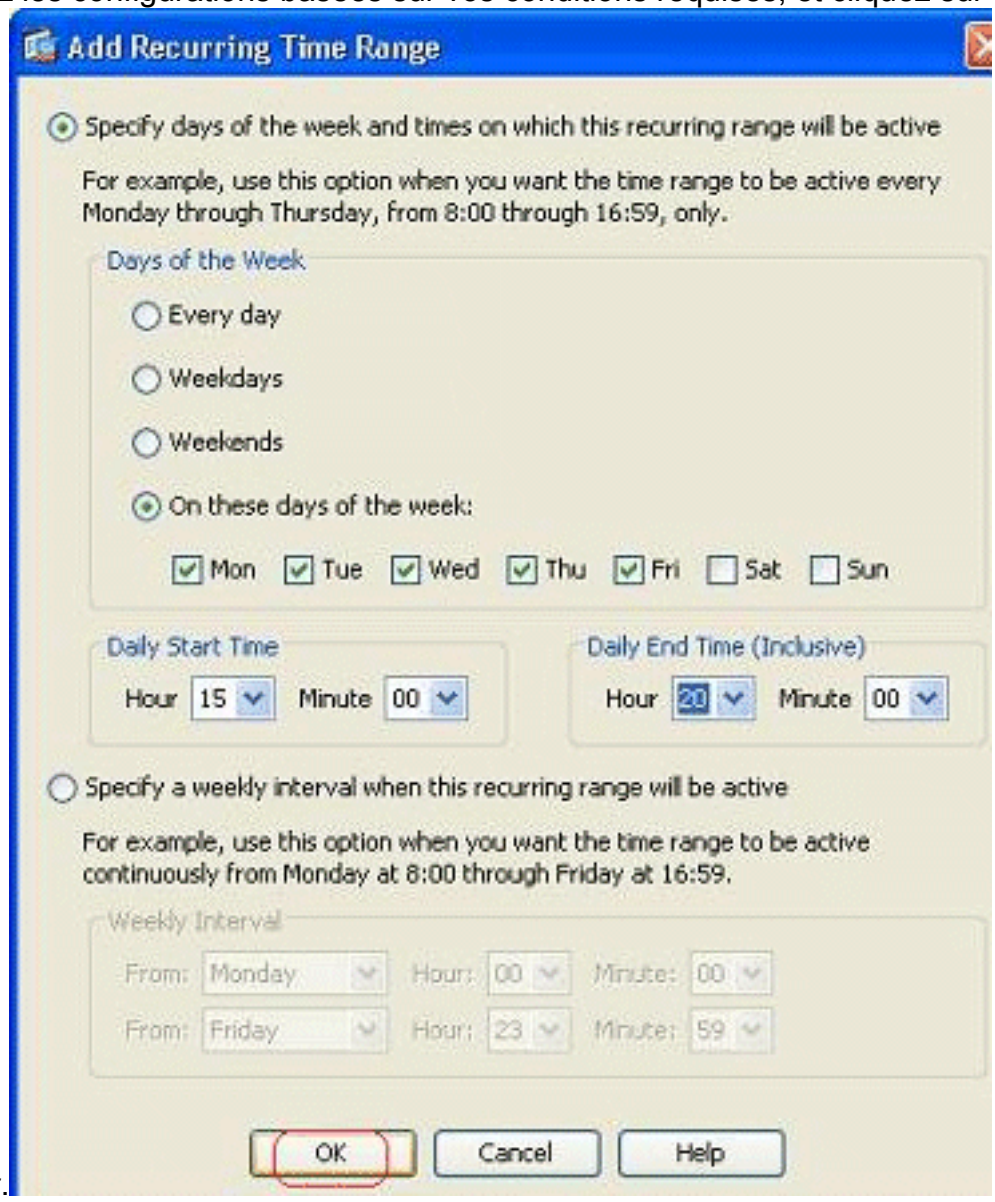
d'accès. Selon cette configuration de règle d'accès, l'utilisateur chez 172.16.10.50 a été limité d'utiliser toutes les ressources du 14h 05/Feb/2011 au 16h30 06/Feb/2011. C'est le CLI équivalent sorti :

```
time-range Restrict-Usage absolute start 14:00 05 February 2011 end 16:30 06 February 2011
! access-list inside_access_out extended deny ip host 172.16.10.50 any time-range Restrict-
Usage ! access-group inside_access_out in interface inside
```

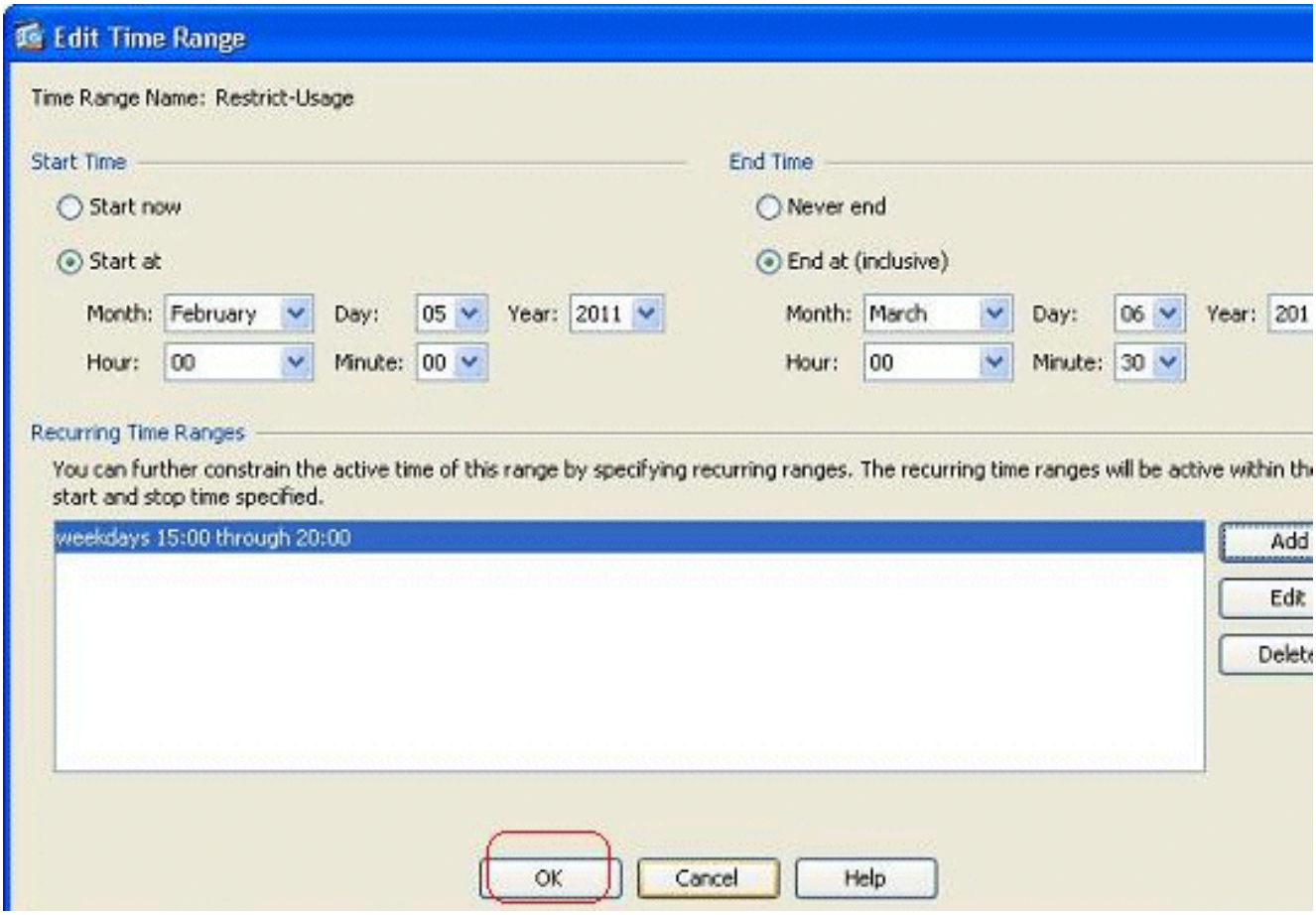
6. Voici un exemple sur la façon dont spécifier une plage de temps récurrente. Cliquez sur Add afin de définir une plage de temps
récurrente.



7. Spécifiez les configurations basées sur vos conditions requises, et cliquez sur OK afin de se terminer.



8. Cliquez sur OK afin de retourner de nouveau à la fenêtre de plage de temps.



Selon cette configuration, l'utilisateur chez 172.16.10.50 a été refusé l'accès à toutes les ressources de 15h à 20h tous les jours de semaine excepté samedi et dimanche.

```
! time-range Restrict-Usage absolute start 00:00 05 February 2011 end 00:30 06 March 2011
periodic weekdays 15:00 to 20:00 ! access-list inside_access_out extended deny ip host
172.16.10.50 any time-range Restrict-Usage ! access-group inside_access_out in interface
inside
```

Remarque: Si une commande de **time-range** a des valeurs absolues et périodiques spécifiées, alors les commandes **périodiques** sont évaluées seulement après que l'heure de début absolue est atteinte, et ne sont pas encore évaluées après l'heure de fin absolue est atteintes.

Informations connexes

- Page de documentation de Cisco ASA
- Support et documentation techniques - Cisco Systems